# A Blockchain Based Framework Secured by ECDSA to Curb Drug Counterfeiting (Un marco basado en blockchain asegurado por ECDSA para frenar la falsificación de medicamentos)

**Abstracto:**

La falsificación de drogas se ha convertido en un problema mundial. El problema de la falsificación se ha vuelto tan grande que ha atraído una atención significativa entre los investigadores y los responsables políticos. La industria de las drogas falsas tiene un valor de 10 mil millones de dólares por año, según lo estimado por 'ASSOCHAM' en 2017. También estimado por la OMS, alrededor de un millón muere por año debido a las drogas falsas. La dispensación de medicamentos falsos es la principal preocupación, especialmente en países en desarrollo como la India. Una de las razones principales en la falsificación de drogas es la cadena de suministro imperfecta. Hay muchas lagunas en nuestra política actual del sistema de gestión de la cadena de suministro de medicamentos. En el escenario actual de la cadena de suministro, la información no se comparte entre las partes durante el proceso de transferencia o se comparte poca o irrelevante información. Una vez que una parte transfiere la droga a otra parte, la primera parte no No sé qué pasa con las drogas allí después. El medicamento falsificado no solo afecta la condición de salud del paciente o la pérdida financiera del fabricante genuino, sino que también representa una seria amenaza para el estado socioeconómico de la sociedad. En este documento, explicamos detalles de la falsificación de medicamentos junto con un pequeño historial de la industria farmacéutica y su impacto en diferentes áreas y también para contrarrestar las falsificaciones utilizando la tecnología Blockchain. Usando la tecnología Blockchain, explicamos aquí cómo agregar trazabilidad, visibilidad y seguridad a la cadena de suministro de medicamentos. Este sistema propuesto hará un seguimiento de los medicamentos desde su origen desde el fabricante hasta el consumidor final. El medicamento falsificado no solo afecta la condición de salud del paciente o la pérdida financiera del fabricante genuino, sino que también representa una seria amenaza para el estado socioeconómico de la sociedad. En este documento, explicamos detalles de la falsificación de medicamentos junto con un pequeño historial de la industria farmacéutica y su impacto en diferentes áreas y también para contrarrestar las falsificaciones utilizando la tecnología Blockchain. Usando la tecnología Blockchain, explicamos aquí cómo agregar trazabilidad, visibilidad y seguridad a la cadena de suministro de medicamentos. Este sistema propuesto hará un seguimiento de los medicamentos desde su origen desde el fabricante hasta el consumidor final. El medicamento falsificado no solo afecta la condición de salud del paciente o la pérdida financiera del fabricante genuino, sino que también representa una seria amenaza para el estado socioeconómico de la sociedad. En este documento, explicamos detalles de la falsificación de medicamentos junto con un pequeño historial de la industria farmacéutica y su impacto en diferentes áreas y también para contrarrestar las falsificaciones utilizando la tecnología Blockchain. Usando la tecnología Blockchain, explicamos aquí cómo agregar trazabilidad, visibilidad y seguridad a la cadena de suministro de medicamentos. Este sistema propuesto hará un seguimiento de los medicamentos desde su origen desde el fabricante hasta el consumidor final. Explicamos detalles de la falsificación de medicamentos junto con un poco de historia de la industria farmacéutica y su impacto en diferentes áreas y también para contrarrestar las falsificaciones utilizando la tecnología Blockchain. Usando la tecnología Blockchain, explicamos aquí cómo agregar trazabilidad, visibilidad y seguridad a la cadena de suministro de medicamentos. Este sistema propuesto hará un seguimiento de los medicamentos desde su origen desde el fabricante hasta el consumidor final. Explicamos detalles de la falsificación de medicamentos junto con un poco de historia de la industria farmacéutica y su impacto en diferentes áreas y también para contrarrestar las falsificaciones utilizando la tecnología Blockchain. Usando la tecnología Blockchain, explicamos aquí cómo agregar trazabilidad, visibilidad y seguridad a la cadena de suministro de medicamentos. Este sistema propuesto hará un seguimiento de los medicamentos desde su origen desde el fabricante hasta el consumidor final.

**Publicado en:**[2019 Décima Conferencia Internacional sobre Tecnologías de Computación, Comunicación y Redes (ICCCNT)](https://ieeexplore.ieee.org/xpl/conhome/8932651/proceeding)

**Fecha de la conferencia:** 6-8 de julio de 2019

**Fecha añadida a IEEE *Xplore* :** 30 de diciembre de 2019

**Información del ISBN:**

**Número de** registro de **INSPEC:** 19277639

**DOI:**[10.1109 / ICCCNT45670.2019.8944772](https://doi.org/10.1109/ICCCNT45670.2019.8944772)

**Editorial:**IEEE

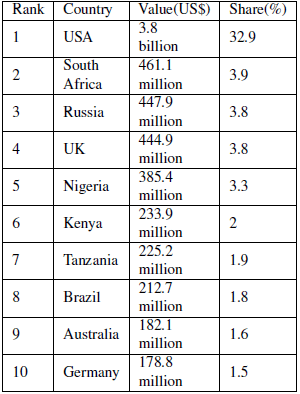
**Lugar de la conferencia:** Kanpur, India, India

**SECCIÓN I.**

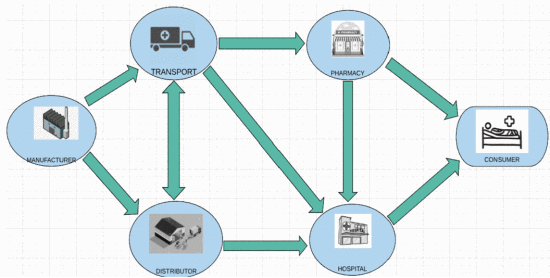
## **Introducción**

Imagine una situación en la que su hijo sufre alguna enfermedad peligrosa. Los síntomas incluyen dolor de cabeza, sudoración, vómitos y fiebre. Ha llevado a su hijo al mejor médico de confianza y le ha administrado el medicamento recetado por el médico. Entonces ahora te sientes un poco relajado. Pero el estado de salud de su hijo no mejora o incluso se deteriora o, peor aún, su hijo muere, porque el medicamento en el que ha confiado es falso. No es una posibilidad distante, esto es real para la mayoría de los países en desarrollo, incluso para algunos países desarrollados. A nivel mundial, los medicamentos falsos son un problema multimillonario. Desde el tamaño, la forma y el color de los productos farmacéuticos, hasta el envase se ven exactamente como los reales, estos resultados fraudulentos generalmente contienen pequeñas cantidades de los elementos activos o incluso ninguno en absoluto o, peor aún, algunos ingredientes fatales. Es muy triste, pero el hecho es que India es el centro épico de fabricación de medicamentos falsos. No hay duda de que estos medicamentos falsos representan un grave peligro para los consumidores y la industria farmacéutica. Por lo tanto, es necesaria la visibilidad en tiempo real de la producción y gestión de medicamentos. Blockchain[1] es la respuesta para tratar con medicamentos falsificados, ya que está abierto a todos y las transacciones almacenadas en formato de libro mayor digital manteniendo la seguridad y la privacidad de los usuarios de forma distribuida [2] .

**Tabla I:** Los 10 principales países importan drogas de la India en 2017-18 [3]



El concepto de tecnología Blockchain provino de bitcoin cryp-tocurrency [4] donde no se requiere un tercero para la transacción. En Blockchain, las transacciones se llevan a cabo en un sistema distribuido de igual a igual. Ha sido un pensamiento común que Blockchain es solo para el sector financiero, ya que se basa en la idea de bitcoin. El verdadero potencial de Blockchain ha salido a la luz en los últimos años. La plataforma descentralizada de la tecnología se puede utilizar en muchas aplicaciones prácticas [5], tales como atención médica, logística, Internet de las cosas (IoT), sistema de reputación, servicio público, cadena de suministro que están más allá del sector financiero. Si solo el sector sanitario [6] se considera que se puede dividir en muchas partes Gestión de registros médicos, Control de acceso a datos de atención médica, Ensayos clínicos, Gestión de suministro de medicamentos, adjudicación de reclamos de seguro, etc.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8932651/8944341/8944772/10th_ICCCNT_2019_paper_385-fig-1-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8932651/8944341/8944772/10th_ICCCNT_2019_paper_385-fig-1-source-large.gif)

**Figura 1:** Diagrama de arquitectura distribuida del sistema de cadena de suministro de medicamentos.

El resto del documento está organizado de la siguiente manera. La Sección II describe los desafíos en la cadena de suministro que plantean los medicamentos falsos junto con algunos antecedentes de la industria farmacéutica. La solución de Blockchain se discute en la Sección III . En la Sección IV y V se proporciona un modelo propuesto y firma digital por ECDSA. Las secciones VI concluyen el documento discutiendo los resultados observados por el modelo propuesto y los alcances futuros para mejorar.

**SECCION II.**

## **Desafíos en la cadena de suministro de drogas falsas**

El objetivo principal de la industria farmacéutica es descubrir, desarrollar, producir y comercializar medicamentos. Los medicamentos pueden usarse para muchos propósitos, como medicamentos para curar pacientes, vacunación y aliviar cualquier tipo de síntomas. Las compañías farmacéuticas generalmente se ocupan de dos tipos de medicamentos, medicamentos genéricos o de marca. Las compañías farmacéuticas también se ocupan de dispositivos médicos hasta cierto punto. Antes de continuar con las discusiones, necesitamos saber qué son exactamente los medicamentos falsificados y cómo se originaron y cómo encuentran un lugar en la cadena principal de la cadena de suministro de medicamentos. Un medicamento que se compone de los ingredientes activos incorrectos, los componentes activos adecuados a la dosis incorrecta o ninguno de los ingredientes activos prescritos, entonces puede denominarse como un medicamento falsificado. Como sabemos, más de un tercio de las drogas espurias que se producen a nivel mundial tienen su origen en la India, lo que erosiona la reputación de nuestro país en el mercado internacional. ¿Cómo encuentran las drogas falsas una porción tan grande de participación en el mercado? Existen múltiples puntos de contacto que no son seguros y no tienen fundamento, cualquiera de los cuales podría ser un punto de entrada de medicamentos falsificados. Hay algunas razones que se pueden señalar:

* La cadena de suministro global del mercado de drogas es tan compleja que es muy difícil tomar una decisión sobre las drogas o sus ingredientes.
* Cadena de suministro fragmentada (antes de la llegada a su destino final, a veces no pasan las drogas a través de varias compañías comerciales que generalmente no verifican la calidad)
* Uno o varios miembros de la cadena de suministro pueden estar corruptos: adulterar, reemplazar o etiquetar mal los productos en la cadena de suministro.
* Fuente no certificada de materia prima. (Un fabricante de confianza puede ignorar que los ingredientes posiblemente provienen de una fuente no verificada).
* Los fabricantes de medicamentos falsos o las marcas de medicamentos falsos se crean con éxito como compañías farmacéuticas legales y marcas de medicamentos de renombre con la ayuda del papeleo falso.
* Falta de conciencia del consumidor y alto precio de la medicina genuina.
* Ley de aplicación débil de la legislación sobre corrupción y método avanzado utilizado en la falsificación.

Con múltiples puntos de entrada y tantas lagunas y la ausencia de un sistema de seguridad transparente y robusto, para rastrear la cadena de suministro de medicamentos, es un desafío inmenso. Los obstáculos al presente sistema de cadena de suministro se pueden describir como:

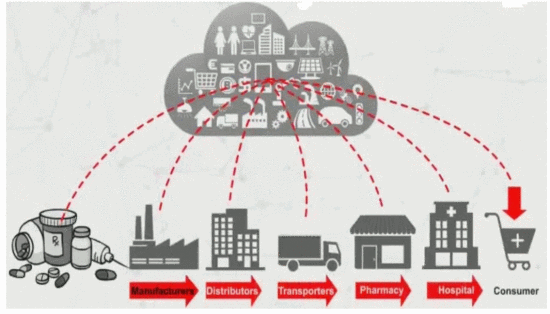
* Ausencia de etiquetado unificado e interoperable e identificaciones estándar.
* Infraestructura de la cadena de suministro sucia, fracturada y opaca. No existe una manera fácil y clara de rastrear el recorrido del producto en la cadena de suministro que pueda revelar el origen real y los puntos de entrega.
* Monitoreo y gestión inadecuados del suministro de la cadena de frío.
* Transferencias entre varias partes, incluidas las empresas de embalaje y de transporte, ya que los medicamentos se transfieren entre múltiples etapas, que podrían ser los posibles puntos de entrada de drogas espurias.
* Diferentes sistemas han sido adoptados por diferentes fabricantes. Esto lleva a un problema compatible donde los distribuidores y las agencias de transporte mantienen diferentes tipos de soluciones a lo largo de sus sistemas de cadena de suministro. Lo que puede causar una confusión en la información o la entrega de los medicamentos y, finalmente, un riesgo para el consumidor.

**SECCION III.**

## **Blockchain la solución**

Dondequiera que los productos estén sujetos a un sistema de producción sensible y donde la reputación considerable y los problemas de responsabilidad significativos se integren con el producto final, las utilidades de Blockchain [7] son obvias. Por lo tanto, la investigación, el desarrollo y la fabricación de medicamentos en el campo farmacéutico es un dominio adicional de implementación para la tecnología Blockchain. [8] [9]

El marco de trabajo descentralizado de Blockchain [10]Además del libro mayor digital distribuido que registra y transfiere datos de manera segura, transparente y rápida. Una cadena de suministro de medicamentos basada en Blockchain dependerá de una red confiable dirigida por Blockchain e IoT. Las entidades o nodos requeridos de la red Blockchain son el fabricante, los distribuidores, las agencias de transporte y el farmacéutico u hospital. Se crea una cadena de suministro que incluye a todas las partes interesadas, como proveedores, vendedores, distribuidores y farmacias, hospitales, etc. Los frascos de medicamentos están etiquetados con números de serie y una huella digital única de su fabricante. Las botellas de drogas empaquetadas para el transporte y los paquetes también contienen los números de serie de las drogas en su interior. Los números de serie escaneados en cada punto de su viaje desde el fabricante hasta el consumidor y la información registrada en Blockchain.[11] Todo el viaje de la droga es visible para todas las entidades en Blockchain. Las entradas de fabricación, como los ingredientes químicos y otros parámetros, pueden actualizarse y vincularse al número de serie de los productos. Entonces, cuando finalmente el consumidor compre el medicamento simplemente escaneando la etiqueta con un teléfono inteligente, él / ella podrá saber todo sobre el medicamento.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8932651/8944341/8944772/10th_ICCCNT_2019_paper_385-fig-2-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8932651/8944341/8944772/10th_ICCCNT_2019_paper_385-fig-2-source-large.gif)

**Figura 2:** Movimiento de drogas en el sistema de la cadena de suministro.

Además, los detalles censurados como la temperatura, la humedad y la ubicación se pueden registrar utilizando sensores inalámbricos y GPS conectados a los paquetes. Como cada información se documenta en el libro mayor compartido, el viaje se hace visible para todas las entidades interesadas. La posibilidad de alterar o modificar el registro ahora es casi imposible. A medida que un producto progresa en la cadena de suministro cruzando varios puntos, se capturará cada transacción o transferencia. Se crea un historial permanente de transacciones del producto desde el punto de fabricación hasta la venta. Este sistema tendrá un registro digital de cada cambio de mano que es completamente resistente a la manipulación. Este sistema impulsado por Blockchain permitiría una forma radical de disminuir los retrasos en el tiempo, los altos costos y los errores humanos que han sido obstáculos para las transacciones,

Podemos extender el marco de Blockchain a pacientes / consumidores que consumen drogas. Se ha trabajado en algunas empresas que dispensarán medicamentos a los pacientes. Los dispensadores que se pueden conectar a la identidad digital del paciente e informar la ingesta de medicamentos al médico, prescriptor o compañía de seguros a través de un dispositivo de sensor inalámbrico incorporado vinculado a Blockchain. Cuando el paciente se olvida de tomar un medicamento importante a tiempo o si está tomando más medicamento del recomendado, se puede enviar un mensaje de alerta a las partes apropiadas (como familiares o asistentes) para que intervengan.

**SECCION IV.**

## **Un modelo propuesto**

Básicamente podemos dividir toda la cadena de suministro de medicamentos desde los fabricantes hasta los consumidores en 6 partes.

1. Fabricante
2. Distribuidor
3. Transportador
4. Farmacia
5. Hospital
6. Consumidor

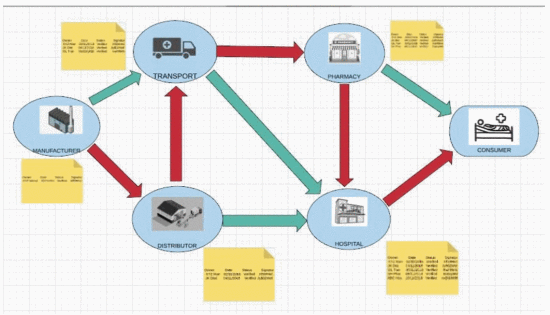
En el modelo de cadena de suministro normal (sin Blockchain), hemos mostrado cómo fluye el medicamento desde el punto de partida, el fabricante hasta el punto final, el consumidor. El modelo se puede describir a continuación.

El fabricante envía los medicamentos al distribuidor oa la agencia de transporte según sus requisitos. El distribuidor puede recoger directamente los medicamentos del fabricante o solicitarlos a través de una agencia de transporte. El distribuidor envía medicamentos nuevamente a hospitales y farmacias a través de las agencias de transporte. Si el requisito del Hospital es muy grande, puede ordenar directamente al Fabricante a través de la agencia de transporte o puede recoger medicamentos directamente del distribuidor. Los hospitales más pequeños pueden ordenar medicamentos de sus farmacias cercanas. Finalmente, el consumidor o paciente obtendrá los medicamentos del Hospital o de la farmacia.

Excluyendo a la última parte (el consumidor), se puede crear un marco Blockchain entre las primeras cinco partes. Es una pregunta obvia que ¿por qué la última parte se ha mantenido fuera de Blockchain? Sabemos que todos los nodos en el marco de Blockchain participan en el proceso de verificación de transacciones. La comunidad de consumidores es muy diversa, desde analfabetos hasta altamente educados, desde niños de secundaria hasta adultos mayores. desde una persona que vive en áreas remotas hasta la persona que vive en ciudades, por lo que no todos pueden participar en el procedimiento de verificación de transacciones. Y también una cosa más es que si agregaremos a todos los consumidores al marco de Blockchain, entonces el sistema estará muy cargado, ya que hay miles de millones de consumidores en nuestra nación. Gestionar datos tan grandes será costoso y la complejidad también aumentará. Puede que en un futuro cercano todos los consumidores puedan ser parte de Blockchain, pero por ahora estamos manteniendo al consumidor fuera de Blockchain. Pero hay una plataforma donde cada consumidor puede verificar la autenticidad del medicamento, se discutirá más adelante en esta sección.

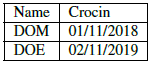
Como ya hemos discutido que nuestro sistema tradicional consiste en algunos agujeros de bucle, crearemos un marco de Blockchain descentralizado con un libro mayor distribuido compartido con las cinco entidades. Cada entidad debe verificarse antes de agregarlas al marco de Blockchain.

Primero, todos los fabricantes de medicamentos deben estar certificados por la CDSCO (Organización Central de Control de Medicamentos) India. Cada fabricante debe tener una identificación única. El fabricante del medicamento debe ser una entidad confiable. Tiene que asegurarse de que todo el fabricante registrado produzca medicamentos genuinos y que el Gobierno de la India debe asumir la responsabilidad de la autenticidad. Si los fabricantes genuinos producen medicamentos falsos, será imposible detener la falsificación con nuestro marco de Blockchain propuesto. Una vez que se produce un medicamento, debe estar etiquetado por la identificación única de los fabricantes, el nombre del medicamento y la composición del medicamento y otros detalles. El fabricante también tiene que poner una huella digital holográfica única en el paquete del medicamento utilizando su identificación única que será difícil de copiar. La información del medicamento se agrega al libro mayor compartido con todos los detalles del medicamento. Ahora el fabricante transferirá los medicamentos al distribuidor. Todos los distribuidores registrados en Blockchain también deben tener asignada una identificación única. Durante la transferencia de los fabricantes al distribuidor, ambas partes deben firmar digitalmente utilizando sus claves privadas en el libro mayor distribuido y la transacción se agrega al bloque. Y todas las entidades en Blockchain deben verificar la transacción antes de agregar otra transacción. Para que nadie pueda negar o alterar esta transacción en el futuro. Ahora, el único objetivo del distribuidor es distribuir los medicamentos de acuerdo con los requisitos de los hospitales y tiendas de farmacia a través de agencias de transporte. Una vez que el distribuidor recibe los medicamentos del fabricante, todas las partes en Blockchain sabrán que el distribuidor ha recibido los medicamentos. La agencia de transporte ahora llevará los medicamentos del distribuidor a las farmacias y hospitales. La transferencia entre el distribuidor y las agencias de transporte ocurrirá después de que ambos firmen digitalmente en el libro mayor compartido usando sus claves privadas. Es un período crucial durante el transporte porque durante el transporte la probabilidad de falsificación es máxima. Aquí podemos tomar la ayuda de IoT y dispositivos sensores inalámbricos para rastrear y verificar. La transferencia entre el distribuidor y las agencias de transporte ocurrirá después de que ambos firmen digitalmente en el libro mayor compartido usando sus claves privadas. Es un período crucial durante el transporte porque durante el transporte la probabilidad de falsificación es máxima. Aquí podemos tomar la ayuda de IoT y dispositivos sensores inalámbricos para rastrear y verificar. La transferencia entre el distribuidor y las agencias de transporte ocurrirá después de que ambos firmen digitalmente en el libro mayor compartido usando sus claves privadas. Es un período crucial durante el transporte porque durante el transporte la probabilidad de falsificación es máxima. Aquí podemos tomar la ayuda de IoT y dispositivos sensores inalámbricos para rastrear y verificar.[12]Se puede conectar un sistema GPS al paquete de medicamentos y se puede monitorear constantemente antes de que llegue a su próximo destino. También se puede colocar un sensor inalámbrico dentro del paquete que controlará constantemente la temperatura, la humedad y otros parámetros porque algunos medicamentos son sensibles a la temperatura y una temperatura más alta estropeará el medicamento. De manera similar, se realiza la transferencia de medicamentos entre la agencia de transporte y el hospital o la agencia de transporte y la farmacia. Después de recibir y verificar los medicamentos, la agencia de transporte y el hospital deberán firmar digitalmente con sus claves privadas. Ahora el medicamento ya está disponible para su uso final. Los medicamentos ahora se pueden administrar a los pacientes o los consumidores pueden comprar en las farmacias. Volviendo al consumidor o la parte final del sistema Blockchain. Como hemos mantenido a la parte final fuera de Blockchain, ¿cómo pueden estar seguros de que los medicamentos que han comprado son genuinos? Se puede crear una plataforma en la nube del sistema Blockchain con algún control de acceso donde todos los detalles del medicamento se almacenan durante todo su recorrido desde el fabricante hasta el consumidor. Simplemente escaneando un código QR o ingresando un número de serie único en el paquete del medicamento, el consumidor podría conocer todos los detalles de un medicamento desde su origen hasta el usuario final.

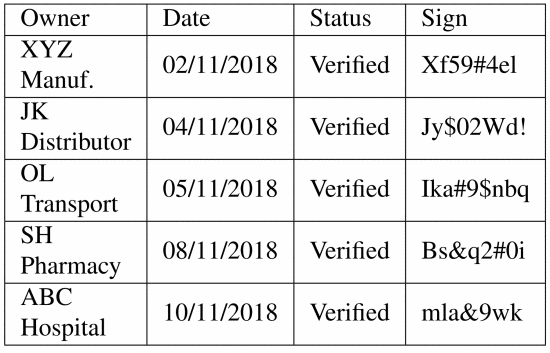
[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8932651/8944341/8944772/10th_ICCCNT_2019_paper_385-fig-3-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8932651/8944341/8944772/10th_ICCCNT_2019_paper_385-fig-3-source-large.gif)

**Fig. 3:** Arquitectura de la cadena de suministro de medicamentos basada en blockchain

**Tabla II:** detalles del medicamento

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8932651/8944341/8944772/10th_ICCCNT_2019_paper_385-table-2-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8932651/8944341/8944772/10th_ICCCNT_2019_paper_385-table-2-source-large.gif)

**Tabla III:** detalles de la transacción

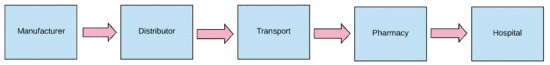
[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8932651/8944341/8944772/10th_ICCCNT_2019_paper_385-table-3-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8932651/8944341/8944772/10th_ICCCNT_2019_paper_385-table-3-source-large.gif)

**SECCION V.**

## **Firma y verificación por ECDSA**

Las curvas elípticas (EC) es un método moderno que se ha convertido en un área importante de investigación en criptografía de clave asimétrica / clave pública. Esta criptografía se basa en campos finitos en la estructura algebraica de curvas elípticas. En general, la criptografía de curva elíptica utiliza claves de menor tamaño en comparación con la criptografía no EC para proporcionar el mismo nivel de seguridad. El algoritmo de firma digital de curva elíptica (ECDSA) es una variante del algoritmo de firma digital (DSA) que utiliza claves derivadas de curvas elípticas. [13]

Como en el modelo propuesto, se ha asumido que el medicamento fluye a través de los nodos marcados con una flecha roja. [14] [15] Para simplificar, el diagrama se puede volver a dibujar a continuación:

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8932651/8944341/8944772/10th_ICCCNT_2019_paper_385-fig-4-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8932651/8944341/8944772/10th_ICCCNT_2019_paper_385-fig-4-source-large.gif)

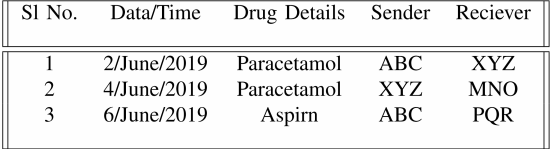
**Fig. 4:** Flujo de drogas

Como el consumidor / paciente ha quedado excluido del marco de Blockchain, también permanecerá fuera del DSA de la CE. Básicamente durante el transporte de drogas ocurren dos procesos en cada transacción:

1. Un nodo envía.
2. Otro nodo recibe.

Por lo tanto, para garantizar una autenticación del 100%, tanto el receptor del remitente debe iniciar sesión digitalmente en el libro mayor compartido. [16] Consideremos la primera letra como sus nombres: MDTPH

**Tabla IV:** Libro mayor compartido

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8932651/8944341/8944772/10th_ICCCNT_2019_paper_385-table-4-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8932651/8944341/8944772/10th_ICCCNT_2019_paper_385-table-4-source-large.gif)

Para garantizar una autenticación robusta y libre de falsificaciones, se utiliza el algoritmo de firma digital de curva elíptica [17] en el marco de Blockchain para la firma y verificación.

Como hay 5 nodos, todos deben estar de acuerdo en 3 cosas / parámetros para garantizar que el DSA EC funcione correctamente:

1. mipag( a , b ) , p > 3, Una curva elíptica
2. PAG∈ Epag( a , b ), Un punto de la curva tal que O ( P) = n , n es un numero primo
3. Una función hash h

Esta información debe estar disponible para todos los nodos del marco Blockchain. Después de este proceso, todos los nodos deben calcular sus claves de forma independiente y por separado.

### A. Generación clave

#### 1) fabricante

* Elige un entero unametro, ( 1 < ametro< n )
* Calcular Qmetro= ametro. PAG
* *PublicKeyforManufacturer:* ( Epag( a , b ) , P, Qmetro, n , h )
* *PrivateKeyforManufacturer* :unametro

#### 2) Distribuidor

* Elige un entero unare, ( 1 < are< n )
* Calcular Qre= are. PAG
* *PublicKeyforDistributor:* ( Epag( a , b ) , P, Qre, n , h )
* *PrivateKeyforDistributor* :unare

De esta forma, se pueden generar las claves públicas y privadas para Transporte, Farmacia y Hospital.

Como cada nodo está seleccionando su clave privada de forma independiente, existe la posibilidad de que la misma clave sea elegida por dos nodos. Por lo tanto, para garantizar la no redundancia, se deben hacer dos cosas:

1. Un algoritmo aleatorio para elegir un número del intervalo 1 a n.
2. Se debe elegir una n grande para garantizar una distribución uniforme de números aleatorios.

Después del proceso de generación de claves, el proceso de firma en cada transacción continuará hasta que el medicamento llegue al usuario final / hospital. Después de completar cada transacción, debe haber dos firmas digitales, tanto del remitente como del receptor, y el receptor debe firmar después de recibir los medicamentos recetados; si falta uno, la transacción debe cancelarse o informarse como no válida.

### B. Firma

Considere la primera transacción en la que el fabricante envía el medicamento al distribuidor:

[[Fig. 5: - Fabricante a distribuidor](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8932651/8944341/8944772/10th_ICCCNT_2019_paper_385-fig-5-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8932651/8944341/8944772/10th_ICCCNT_2019_paper_385-fig-5-source-large.gif)

**Fig. 5:** Fabricante a distribuidor

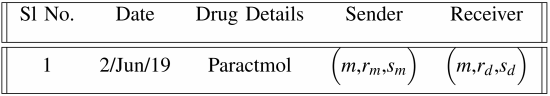
#### 1) Firmar por remitente Fabricante

* El remitente selecciona un entero kmetro, ( 1 < kmetro< n )
* Calcular Rmetro= kmetro. PAG
* Calcular rmetro= x ( m o dn )
* Si rmetro= 0, Seleccione otro k
* Calcular: Smetro= k- 1metro( h ( m ) + ametro. rmetro) (mod n)
* La firma del fabricante es: ( m , rmetro, smetro)

#### 2) Firmar por el distribuidor receptor

* El remitente selecciona un entero kre, ( 1 < kre< n )
* Calcular Rmetro= kre. PAG
* Calcular rre= x ( m o dn )
* Si rre= 0, Seleccione otro k
* Calcular: Sre= k- 1re( h ( d) + are. rre)( *modn* ) • La firma del distribuidor es:( m , rre, sre)

**Tabla V:** Libro mayor compartido actualizado

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8932651/8944341/8944772/10th_ICCCNT_2019_paper_385-table-5-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8932651/8944341/8944772/10th_ICCCNT_2019_paper_385-table-5-source-large.gif)

Ahora todos los nodos en el marco de Blockchain pueden verificar que el Fabricante 'm' haya enviado 100 tiras de Paracetamol al Distribuidor 'd' y al Distribuidor 'd' recibido con éxito.

### C. Verificación

Verificación por cualquier Farmacia decir:

#### 1) Verificación de la firma del remitente

* Firma del remitente: ( m , rmetro, smetro)
* Clave pública para el remitente: ( Epag( a , b ) , P, Qmetro, n , h )
* Pharamcy calcula:

u = h ( m ) . S- 1metro( m o dn )v = rmetro. S- 1metro( m o dn )u . PAG+ v . Qmetro=( x∗, y∗)r∗= x∗( m o dn )

Ver fuenteRight-click on figure for MathML and additional features.

* Si rmetro= r∗

Es el auténtico signo del fabricante.

#### 2) Verificación de la firma del receptor

* Firma del remitente: ( m , rre, sre)
* Clave pública para el remitente: ( Epag( a , b ) , P, Qre, n , h )
* Pharamcy calcula:

u = h ( m ) . S- 1re( m o dn )v = rre. S- 1re( m o dn )u . PAG+ v . Qre= ( x∗, y∗)r∗= x∗( m o dn )

Ver fuenteRight-click on figure for MathML and additional features.

* Si rre= r∗

Es el auténtico signo de distribuidor.

Ahora, como ambos signos se verificaron con éxito, cualquier nodo en el marco de Blockchain puede concluir que el fabricante 'm' había enviado 100 tiras de Paracetamol al distribuidor 'd' el 5 de mayo de 2019 a las 15:30 en Bhubaneswar y el distribuidor 'd' recibió con éxito.

Ahora, supongamos que un Distribuidor malicioso intenta enviar un Asprin que no vino de un Fabricante original a un transportista. Entonces, cuando comience la transacción, el transportista y otros nodos pueden verificar que el distribuidor no recibió ningún 'Asprin' de ningún fabricante. Entonces la transacción será cancelada.

Este proceso de verificación se puede automatizar donde el marco mismo puede verificar si un medicamento enviado por un remitente ya ha recibido de un nodo. Si no, la transacción no debería iniciarse en absoluto y se puede detectar el nodo malicioso.

Consideremos los agujeros de bucle donde pueden ingresar medicamentos falsificados en la cadena de suministro. Considere un caso en el que una entidad maliciosa intenta reemplazar o agregar algunos medicamentos falsos, etiquetados como el fabricante original. Agregar medicamentos falsos es totalmente imposible ya que los medicamentos falsos no son producidos por un fabricante registrado que no puede firmar digitalmente en el libro mayor. Como el reemplazo es una posibilidad, asuma un caso: de alguna manera, una entidad maliciosa logra reemplazar algunos medicamentos genuinos con algunos falsos. ¿Qué hará esa entidad con los medicamentos genuinos reemplazados, dónde venderlos? Por lo general, las drogas genuinas cuestan más que las drogas falsas. La venta de un medicamento de menor costo a un precio más alto es fácil, pero no es deseable. En el peor de los casos, si ese medicamento encuentra algún camino hacia una farmacia, simplemente escaneando el código QR, un ciudadano normal puede ver que la cadena de suministro no está completa o fragmentada. A medida que cada transacción se actualice a través de un libro compartido distribuido y se firme digitalmente, cualquier cambio en cualquier transacción será visto por todos y se identificará una entidad maliciosa.

**SECCION VI.**

## **Conclusión**

Con el reciente avance en las tecnologías de red e internet, existe una necesidad urgente de mejorar los servicios de atención médica. En este documento se han discutido varios temas relacionados con la gestión de la cadena de suministro de medicamentos y cómo Blockchain puede prevenir los problemas de manera transparente y segura con el uso extensivo del algoritmo de firma digital de curva elíptica (ECDSA). Aquí, también se ha descrito cómo se puede usar Blockchain para agregar trazabilidad y visibilidad a la cadena de suministro de medicamentos para superar los problemas de la falsificación de medicamentos. Se ha presentado un modelo de arquitectura descentralizada de Blockchain con un sistema de contabilidad compartida, que no solo evitará la falsificación de medicamentos, sino que también hará que el suministro de medicamentos sea más robusto, transparente y confiable. El uso de ECDSA proporciona un proceso seguro muy robusto para la autenticación de las firmas por las partes participantes. Usando este modelo propuesto, podemos bloquear las lagunas en nuestra cadena de suministro de medicamentos actual.

En el futuro, el marco se puede mejorar aún más al agregar a todos los consumidores a Blockchain, lo que podría ser una tarea difícil para el almacenamiento de datos. El contrato inteligente [18] también se puede implementar para eliminar al intermediario entre los pacientes y los fabricantes, lo que finalmente beneficiará a los consumidores.

Además, nuestro modelo propuesto de marco Blockchain no solo se limita a contrarrestar la falsificación de medicamentos, sino que también será útil en el seguimiento en tiempo real, como la entrega programada de productos.