ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA EN SISTEMAS

UNIDAD DE TITULACIÓN

Diseño de Sistema Criptográficamente Seguro de Dinero Electrónico

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL GRADO DE MAGISTER EN SOFTWARE CON MENCIÓN SEGURIDADES

VARGAS SALAZAR MÓNICA PATRICIA
monica.vargas@epn.edu.ec

Director: PhD. ENRIQUE MAFLA
enrique.mafla@epn.edu.ec

Febrero 2020

APROBACIÓN DEL DIRECTOR

Como director del trabajo de titulación, Diseño de Sistema Criptográficamente Seguro para Dinero Electrónico, desarrollado por Vargas Salazar Mónica Patricia, estudiante de la Maestría de Software con Mención en Seguridades; habiendo supervisado la realización de este trabajo y realizado las correcciones correspondientes, doy por aprobada la redacción final del documento escrito para que prosiga con los trámites correspondientes a la sustentación de la Defensa oral.

PhD. Enrique Mafla

DIRECTOR

DECLARACIÓN DE AUTORÍA

Yo, Mónica Patricia Vargas Salazar, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Mónica Patricia Vargas Salazar

DEDICATORIA

A mis abuelitas, pilares de amor, dedicación y constancia; a mi familia. A mi mejor amiga y a mis angelitos que se me adelantaron, con todo mi corazón.

AGRADECIMIENTO

A Dios, que siempre me ha acompañado a lo largo de toda mi vida.

A mis abuelitas, por darme el ejemplo de que todo es posible.

A mis padres, por ser mi soporte en cada idea, aunque a veces salen de la cordura. Todo lo que emprendo es gracias a su apoyo.

A mis hermanas, a quienes admiro mucho por su entrega. Todas ellas han sido madres excelentes y se han esforzado por culminar sus carreras día a día.

A mi mejor amiga y su familia, quienes con sus consejos siempre me han alentado a seguir adelante.

A mis cuñados, que me han apoyado incondicionalmente.

A mis sobrinos, que me han alentado para ser un ejemplo a seguir.

A mis profesores, en especial a mi tutor, a quién admiro por su don de sabiduría y su paciencia, herramientas que usó como guía para que este proyecto culmine de manera exitosa.

ÍNDICE DE CONTENIDO

APROBACIÓN DEL DIRECTOR 2

DECLARACIÓN DE AUTORÍA 3

DEDICATORIA 4

AGRADECIMIENTO 5

ÍNDICE DE CONTENIDO 6

LISTA DE FIGURAS 9

RESUMEN 12

ABSTRACT 13

1. INTRODUCCIÓN 14

1.1. Pregunta de investigación 15

1.2. Descripción del Problema 15

1.3. Objetivo general 16

1.4. Objetivos específicos 16

1.5. Alcance 17

1.6. Marco Teórico 17

1.6.1 Sistema criptográfico 17

1.6.2 Dinero electrónico 19

1.6.3 Sistema de pago electrónico 20

1.6.4 Herramientas bancarias 22

1.6.5 Legislación vigente en Ecuador 23

1.6.6 ISO 27001 25

1.6.7 COBIT 26

1.6.8 NISTIR 7977 26

2. METODOLOGÍA 27

2.1. Explicación de la metodología 28

2.1.1. Características de la Metodología de Diseño 30

2.2. Análisis de las metodologías de desarrollo de software 32

2.3. Aplicación de la metodología de diseño 34

2.3.1. Fase I: Análisis de Factibilidad 34

2.3.2. Levantamiento de Requerimientos 35

2.4. Métodos y Herramientas de Trabajo 36

2.4.1. Normas Seguridad 37

2.4.2. NIST 38

2.4.3. Herramientas de Contabilidad 41

2.4.4. Hyperledger Fabric 42

2.4.5. Definición de Seguridad 43

2. Diseño 44

2.1. Diseño del sistema 44

2.1.1. Requerimientos del Sistema 44

2.1.2. Infraestructura de red 44

2.1.3. Prototipo del Sistema 46

2.2. Seguridad 59

2 Discusión 60

3 Conclusiones 62

Bibliografía... 62

LISTA DE FIGURAS

Ilustración 1: metodología del diseño Morris Asimov 29

Ilustración 2: metodología diseño Nigel Cross 30

Ilustración 3: herramientas de Hyperledger 41

Ilustración 4: funcionamiento de Red 45

Ilustración 5: funcionamiento del peer 46

Ilustración 6: funcionamiento Libro de Contabilidad 46

Ilustración 7: diagrama casos de uso 47

Ilustración 8: validar y crear Certificado de Autentificación 47

Ilustración 9: cifrar transacción 48

Ilustración 10: gestionar blockchain y replicación 49

Ilustración 11: gestionar reglamento interno 49

Ilustración 12: gestionar reglamento por pedido externo 50

Ilustración 13: secuencia crear Certificado Autentificación 51

Ilustración 14: secuencia cifrar transacción 51

Ilustración 15: secuencia gestionar Blockchain 52

Ilustración 16: secuencia gestión reglamento 52

Ilustración 17: secuencia gestión reglamento interno 53

Ilustración 18: diagrama de despliegue 54

Ilustración 19: flujo de transacción 55

Ilustración 20: Funcionamiento entidades 55

Ilustración 21: Creación usuario 56

Ilustración 22: Usuario en la entidad 56

Ilustración 23: Ingreso en el usuario 56

Ilustración 24: Registro de transacción 57

Ilustración 25: Creación nueva transacción 57

Ilustración 26: Comprobación de reglamento 58

Ilustración 27: Transacción comprobada 58

Ilustración 28: Auditoría de la transacción 59

LISTA DE TABLAS

Tabla 1: aplicación metodología del diseño 30

Tabla 2: Metodologías de desarrollo de software 32

Tabla 3: requerimiento identificar entidad bancaria 35

Tabla 4: requerimiento generación certificado 35

Tabla 5: requerimiento almacenamiento y replicación de transacción 36

Tabla 6: comparación normas 37

Tabla 7: vulnerabilidades mitigadas 59

RESUMEN

El siguiente proyecto presenta un análisis de prototipo del sistema criptográficamente seguro de dinero electrónico, realizando en primera instancia un análisis de las normativas vigentes en Ecuador, lo que conllevó al levantamiento de requerimientos asumiendo que cada institución bancaria cuenta con sus propios sistemas de datos. El proyecto presenta una intercomunicación hipotética entre bancos asegurando las transacciones que se dan entre estas instituciones y proponiendo que sean reguladas por el Banco Central del Ecuador.

El estudio se llevó a cabo utilizando metodología de diseño y normativas NIST, Hyperledger Fabric como herramienta principal, para establecer recomendaciones de vulnerabilidades.

Palabras clave: Hyperledger, Blockchain, chaincode, contratos inteligentes, peer, canales.

ABSTRACT

The project is a prototype analysis that consists on a design of a cryptographically secure system for electronic money, for which the Ecuadorian legislation was applied. This led to raising of requirements by taking into account that each banking institution has its own data system.

This project presents hypothetical intercommunication between banks that protect transactions that take place between these institutions and propose those to be regulated by the Central Bank of Ecuador.

The study was carried out using Design Methodology and NIST Standards, Hyperledger Fabric as the main tool, to stablish recommendations related to vulnerability.

Keywords: Hyperledger, blockchain, chaincode, smart contract, peer, chanel.

1. INTRODUCCIÓN

El inicio de la era de la información ha propiciado que las personas dependan cada vez más de las comunicaciones de red. La tecnología informática ha impactado significativamente en la capacidad de acceder, almacenar y distribuir información. El comercio electrónico se cuenta entre uno de los usos más relevantes de este tipo de tecnología; ya que se puede realizar transacciones financieras a través de información electrónica intercambiada mediante el uso de líneas de telecomunicación. En este contexto, un requisito clave para el comercio electrónico es el desarrollo de un sistema de pago electrónico seguro y eficiente. Adicionalmente, el auge del internet destaca la necesidad de implementar mecanismos de seguridad, dado que la red promete ser un medio líder para el comercio electrónico a futuro.

Los sistemas de pago electrónico se presentan en distintas formas, incluyendo cheques digitales, “tarjetas de débito, tarjetas de crédito y tarjetas de valor almacenado”. Las características de seguridad habituales para tales sistemas son la privacidad, la autenticidad y el no repudio.

Por otro lado, es primordial entender un sistema de información consiste en la interacción de varios componentes software, hardware, humano, aplicaciones y tareas que buscan procesar datos e información (Gonzalez-Longatt, 2012). La criptografía es una técnica para cifrar mensajes, la cual proviene del griego Kryptos que se traduce como escondido (Sgarro, 1990). En consecuencia, un sistema criptográfico seguro es la interacción entre software y hardware que permite encriptar y proteger la información más susceptible.

Debido a la nueva era electrónica se ha optado por el uso de dinero electrónico en Europa, Asia y algunos países de América, principalmente como alternativa de intercambio monetario en negociaciones. No obstante, lo manifestado, con el uso del dinero electrónico conlleva riesgos que es menester considerar, tales como el lavado de activos y la estafa. Por consiguiente, es importante evitar el uso erróneo de esta herramienta mediante operaciones transparentes y el servicio de no repudio. (Bissessar, 2016)

La “Ley Orgánica para la Reactivación de la Economía, Fortalecimiento de la Dolarización y Modernización de la Gestión Financiera”, propuso establecer para Ecuador que los bancos manejen el dinero electrónico a partir del 18 abril del 2019. Además, con el crecimiento de los sistemas de comercio electrónico se ha hecho necesaria la implementación de medios de pago adecuado que sean más rápidas y accesibles.

Es por esta razón que se propone el prototipo de un Sistema Criptográficamente Seguro de Dinero Electrónico, con la finalidad de que las transacciones se realicen con mayor agilidad y calidad; bajo un diseño de sistema de pago electrónico funcional, es decir criptográficamente seguro.

1.1. Pregunta de investigación

¿Puede existir un sistema criptográficamente seguro que cumpla con las normativas ecuatorianas para el manejo de dinero electrónico?

1.2. Descripción del Problema

La mayor parte del sistema bancario soporta transacciones físicas y en línea. Pero el sistema de transacciones de dinero electrónico es cada vez más popular debido al uso generalizado de las compras y la banca basadas en Internet. Es por eso que los bancos ofrecen servicios en línea. En ese caso, la mayor preocupación es la seguridad. Entonces, sin garantía de seguridad en las transacciones, este sistema no puede ser prometedor para el cliente.

Por otro lado, con el uso de dinero electrónico se presentan casos de fraude y uso de este mecanismo para lavado de activos o desarrollo de actividades ilícitas (Bissessar, 2016). Asimismo, hay poca seguridad en el manejo de sistemas de pagos (Hanácek, 2015), y en la integración de todos los sistemas de diferentes entidades bancarias (Syeful, 2015)

Por otro lado, en América Latina se han presentado problemas de ataques cibernéticos en entidades bancarias. En efecto, el informe de “Ciberseguridad en el Sector Bancario en América Latina y el Caribe, en sus principales hallazgos señala lo siguiente” (Organización de los Estados Americanos, 2018):

- Entidades bancarias grandes, medianas y pequeñas fueron objeto de ataques de todo tipo de eventos de seguridad digital.
- Se identificó ocurrencia de eventos de malware diariamente; en entidades bancarias grandes en 40%, medianas en 28% y pequeñas en 9%.
- Fueron víctimas de ataques exitosos; entidades bancarias grandes en 65%, medianas en 43% y pequeñas en 19%
- Cuentan con un plan de comunicaciones “para informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida; entidades bancarias grandes en 77%, medianas en 65% y pequeñas en 56%” (Organización de los Estados Americanos, 2018).

- Reportan los incidentes “sufridos ante autoridad de aplicación de la ley; entidades bancarias grandes en 81%, medianas en 65% y pequeñas en 46%” (Organización de los Estados Americanos, 2018).
- “No están implementando herramientas, controles o procesos usando tecnologías digitales emergentes; entidades bancarias grandes en 26%, medianas en 44% y pequeñas en 67%” (Organización de los Estados Americanos, 2018).

Según las cifras referidas, el crimen por internet aumenta rápidamente; el ataque criminal en varios sistemas en línea hackeó información personal y profesional, intrusión que ha creado desconfianza en los usuarios. Como resultado, el cibercrimen en la banca es alarmante tanto para el cliente como para el banco. Muchos delincuentes intervienen en la base de datos de la Banca al violar la seguridad y robar los datos personales de los clientes (información de la cuenta, detalles de la tarjeta, identificación de usuario, contraseña, etc.) usando medios ilegales. Una vez que los delincuentes obtienen información personal, la cuenta de los usuarios es vulnerable a los ataques. Por consiguiente, el hackeo es una amenaza latente tanto para el banco como para el usuario.

Por otra parte, uno de los problemas que presenta los sistemas de pagos Interbancarios se ve reflejado en el informe “realizado por la Contraloría General del Estado”, en su examen especial realizado al Sistema Interbancario de Pagos, mismo que señala: *“los registros electrónicos correspondientes a 22 expedientes físicos, lo que no refleja la integridad requerida entre la documentación física y la información constante en la base de datos lo que pone en riesgo la confiabilidad de la información”* (Dirección de Auditoría de Tecnología de la Información, 2015).Con base en la información referida en los párrafos precedentes, se propone el desarrollo de un prototipo de un sistema criptográficamente seguro para el manejo de dinero electrónico.

1.3. Objetivo general

Diseñar un sistema criptográficamente seguro que cumpla con las normativas del Estado y estándares de seguridad internacionales aplicados al dinero electrónico

1.4. Objetivos específicos

- Diagnosticar las vulnerabilidades que se presentan en las plataformas tecnológicas de dinero electrónico.
- Diseñar un sistema que garantice la integridad de los datos y transacciones financieras de los usuarios.

- Proteger la confidencialidad de los datos personales y financieros de los usuarios.
- Aplicar los estándares internacionales de seguridad para la protección de dinero electrónico.

1.5. Alcance

En el proyecto se desarrollará un prototipo de sistema criptográficamente seguro de dinero electrónico que busca demostrar la intercomunicación de transacciones interbancarias por medio de un canal cifrado.

El modelo a seguir es el denominado business to business considerado el más apropiado debido a que podría ser implementado en entidades bancarias dando la opción de compatibilidad con varios aplicativos que ocupe cada institución. Además, el prototipo puede ser utilizado como un modelo que refuerce el sistema de pagos interbancario preexistente, manejado actualmente desde el Banco Central del Ecuador con otras instituciones.

El prototipo emplea un libro de contabilidad que puede ser sincronizado con el reglamento establecido por las entidades reguladoras, permitiendo la verificación del cumplimiento de reglas establecidas en cada una de las transacciones. De esta manera, cada transacción es asegurada por medio de encriptación creando una cadena de información bitcoin que puede ser replicada en una base distribuida.

1.6. Marco Teórico

1.6.1 Sistema criptográfico

Para entender lo que es un sistema criptográfico debemos basarnos primero en los algoritmos que se emplean y su historia centrándonos en los utilizados por entidades bancarias. En la década de 1970, se evaluó un algoritmo criptográfico llamado algoritmo Lucifer, ideado por Horst Feistel, y después de algunos cambios en las funciones internas y la reducción del tamaño de la clave de 112 bits a 56 bits, el algoritmo completo que se convirtió en el Estándar de cifrado de datos (DES) y fue publicado en el Registro Federal en 1975 (Dixit, 2017).

Las instituciones financieras comenzaron a usar DES para crear infraestructuras de seguridad de protección de datos codificados binarios, almacenados en sistemas informáticos y también para proteger la transmisión durante las transacciones electrónicas. Pero los piratas informáticos establecieron un programa mediante el cual cualquier persona

con una computadora conectada a Internet podría penetrar una parte de los recursos de su computadora.

Entonces el nuevo algoritmo entró en escena. Había dos algoritmos principales para reemplazar DES. Triple DES (a veces llamado TDES o 3DES), o estándar de cifrado avanzado. 3DES usa el algoritmo DES original tres veces para cifrar los datos. Utilizando dos o tres claves DES de 56 bits, en 2002, apareció el AES, “el estándar de cifrado avanzado (AES). En criptografía, el estándar de cifrado avanzado (AES) también se conoce como algoritmo Rijndael. Rijndael es un cifrado de bloque iterado que admite longitud de bloque variable y longitud de clave, especificada como 128, 192 o 256 bits” (Medina Vargas & Miranda Mnedez, 2015).

Murphy y Robshaw introdujeron una alternativa de AES al incorporar AES en un cifrado llamado BES que utiliza operaciones algebraicas. Nicolas Courtois y Joseph Pieprzyk trabajaron en una nueva metodología, descubriendo que AES también se puede escribir como ecuaciones cuadráticas (Dixit, 2017).

Entre las herramientas criptográficas de clave pública más usadas se encuentran las siguientes:

- Funciones unidireccionales. Una función unidireccional es una correspondencia entre dos conjuntos que se puede calcular de manera eficiente en una dirección, pero no en la otra.

  Todos los protocolos de clave pública usan pares de claves. Por esta razón, la criptografía de clave pública a menudo se llama criptografía asimétrica. La criptografía convencional a menudo se llama criptografía simétrica, ya que uno puede cifrar y descifrar con la clave privada, pero no puede hacerlo sin ella.

- Firma e identificación. En un sistema de clave pública, un usuario se identifica demostrando que conoce su clave secreta sin revelarla. Esto se realiza por una operación que utilizando la clave secreta se puede verificar o deshacer utilizando la clave pública. Aplicando el principio de seguridad informática de confidencialidad realizado por medio de la identificación. Si un usuario usa un mensaje además de la clave secreta, está realizando una firma digital en el mensaje. La firma digital desempeña el mismo papel que una firma manuscrita; es decir, identifica al autor del mensaje de una manera que no puede ser repudiada y confirma la integridad del mensaje.

- Función hash, es un mapa de todas las cadenas posibles de bits de cualquier longitud a una cadena de bits de longitud fija. A menudo se requiere que tales funciones estén libres de colisiones; es decir, debe ser computacionalmente difícil encontrar dos entradas que tengan el mismo valor. Si una función hash es unidireccional y sin colisión, se dice que es un hash seguro.

  El uso más común de las funciones hash seguras es en las firmas digitales. Los mensajes pueden tener cualquier tamaño, pero un algoritmo de clave pública determinada requiere trabajar en un conjunto de tamaño fijo. Por lo tanto, se codifica el mensaje y se firma el hash seguro en lugar del mensaje en sí.

1.6.2 Dinero electrónico

El dinero electrónico corresponde a un término en evolución, que posee diferentes significados. En principio implica el uso de redes de computadoras y sistemas digitales de valores almacenados para guardar y transferir dinero. Puede considerar estatus legal oficial o no; puede ser histórico, actual o teórico. *"El principio subyacente del dinero electrónico implica el uso de redes informáticas como Internet y sistemas digitales de valores almacenados"* (Syeful, 2015). Ejemplos de dinero electrónico son: depósitos bancarios, transferencia electrónica de fondos, depósito directo, procesadores de pagos y monedas digitales. "El dinero electrónico puede entenderse como una forma de almacenar y transmitir dinero convencional a través de sistemas electrónicos o como moneda digital que varía en valor y es negociable como moneda por derecho propio. El dinero electrónico es un equivalente digital del efectivo, almacenado en un dispositivo electrónico o de forma remota en un servidor" (Syeful, 2015).

Las transacciones con dinero electrónico se pueden realizar a través de varios dispositivos. Estas transferencias pueden realizarse a tanto a nivel nacional como internacional. Este mecanismo constituye un medio de pago adicional a los ya existentes y busca fortalecer la dolarización siendo incluyente, ágil y seguro para toda la población (Banco Central del Ecuador, 2016). El proyecto de dinero electrónico empezó en el 2014, como mecanismo de inclusión financiera que pretendía reducir la brecha del 40% de población económica multiactiva excluida del sistema financiero. (Acosta-Veliz, Guerra-Tejada, & Viteri-Luque, 2018).

El primer sistema en Ecuador se denominó **EFECTIVO** y requería los siguientes pasos para acceder a una cuenta:

a) Marcado a un número, previamente definido, en el celular.

b) Ingreso de cédula.
c) Confirmación de datos.
d) Recarga de dinero electrónico.
e) Solicitud de recepción de cantidad a entidad bancaria y de permiso de uso de la aplicación

Para el retiro existía un código que se enviaba a través de un mensaje de texto o por medio de un cajero.

La tecnología que utilizaba **EFECTIVO** es la siguiente: POS, ATM, NFC, App, IVR, Web, USSD y SMS. El proyecto obtuvo mayor acogida en tres provincias: Pichincha, Guayas y Manabí (El Telégrafo, 2017); siendo manejado por el Banco Central del Ecuador. Sin embargo, con la "Ley Orgánica para la Reactivación de la Economía, Fortalecimiento de la Dolarización y Modernización de la Gestión Financiera, a partir del 18 de abril del 2018, el funcionamiento pasó a las entidades bancarias privadas con el objetivo de incrementar el número de usuarios" (El Telégrafo, 2017).

Uno de los beneficios del dinero electrónico es el ahorro significativo, según lo señala el Banco Central del Ecuador en su boletín: "Cada año el país requiere 2.000 millones de dólares para satisfacer la demanda de monedas y billetes, lo que tiene un efecto negativo en las reservas internacionales de Ecuador" (Banco Central del Ecuador, 2017). En otros países latinoamericanos, cómo Uruguay y Brasil, se ha estudiado los beneficios de realizar transacciones de dinero electrónico en las actividades cotidianas. En estos países se compara la facilidad de uso declarando que es semejante a las tarjetas de crédito, enfatizando que cada una de las leyes deben aprobarse para la utilización de este sistema, proponiendo que inclusive se realice este proceso en cada país por medio de tarifas establecidas (Cassoni, 2013).

El estudio realizado por Machado, respecto a la implementación de la billetera electrónica en medios de transporte público, en ciudades como Porto Alegre, señala: *"la gestión qué se debe realizar en el manejo de dinero electrónico no solo es en el transporte, sino para otras transacciones que se realizan a diario"* (Machado, 2010). De esta manera, se otorga importancia a los sistemas de dinero electrónico para la aplicación en circunstancias cotidianas.

1.6.3 Sistema de pago electrónico

Los sistemas de pago que utilizan redes de distribución electrónica constituyen una práctica frecuente en el sector bancario y comercial, especialmente para la transferencia

de grandes cantidades de dinero. En las cuatro décadas transcurridas desde su aparición, se han producido importantes desarrollos tecnológicos que, por un lado, han ampliado las posibilidades de los sistemas de pago electrónico y, por otro, han creado nuevas prácticas comerciales y sociales, que hacen que el uso de estos sistemas sea necesario. Estos cambios, naturalmente, han afectado la definición de pagos electrónicos, que evoluciona acorde a las necesidades de cada período.

En su forma más general, *"el término pago electrónico incluye cualquier pago a empresas, bancos o servicios públicos de ciudadanos o empresas, que se ejecutan a través de telecomunicaciones o redes electrónicas utilizando tecnología moderna" (Ministerio de Telecomunicaciones y de la Sociedad de la Información , 2019)*. Es evidente que, con base en esta definición, los pagos electrónicos son los pagos ejecutados por el propio pagador, ya sea un consumidor o una empresa, sin la intervención de otra persona. Además, el pago se realiza a distancia, sin la presencia del pagador en un espacio físico y, naturalmente, no incluye manejo de dinero en efectivo. Al proporcionar dicha definición para el sistema de pago electrónico, el investigador incluye la transferencia de información sobre las cuentas de las partes involucradas en las transacciones de comercio electrónico, así como los medios tecnológicos de los canales de distribución a través de los cuales se ejecutan las transacciones.

El dinero electrónico incluye cuatro sistemas diferentes:

- Sistemas centralizados como por ejemplo: "PayPal, eCash, WebMoney, Payoneer, cashU y Ven de Hub Culture, expenden su moneda electrónica directamente al usuario final. Otros sistemas solo se expenden a través de intercambiadores de divisas digitales de terceros. Algunas monedas comunitarias, como algunos sistemas comerciales de intercambio local (LETS) y el Sistema de intercambio comunitario funcionan con transacciones electrónicas" (Amarasiri & Dias, 2015).
- Sistemas descentralizados. Una criptomoneda es un medio de canje que utiliza la criptografía para asegurar las transacciones y controlar la creación de nuevas unidades. Las criptomonedas son un subconjunto de monedas alternativas, o específicamente de monedas digitales. Bitcoin se convirtió en la primera criptomoneda descentralizada en 2009. Desde entonces, se han creado numerosas criptomonedas. Con frecuencia se denominan altcoins, como una mezcla de alternativas de bitcoin. Las criptomonedas utilizan un control descentralizado en lugar de sistemas centralizados de dinero electrónico y/o banca centralizada. El control descentralizado está relacionado con el uso de la

base de datos de transacciones en cadena de bloques de bitcoin en el rol de un distribuidor distribuido. “La criptomoneda descentralizada es producida por todo el sistema de criptomonedas colectivamente, a una velocidad que se define cuando se crea el sistema y que se conoce públicamente. En los sistemas bancarios y económicos centralizados, las juntas corporativas o los gobiernos controlan el suministro de divisas, imprimiendo unidades de dinero fiduciario o exigiendo adiciones a los libros de contabilidad bancarios digitales” (Amarasiri & Dias, 2015).

- Subsistemas móviles o carteras digitales. “Son aquellas que utilizan la transferencia de pago sin contacto para facilitar el pago fácil y brindar al beneficiario más confianza para no utilizar la billetera electrónica durante una transacción” (Amarasiri & Dias, 2015).
- Sistemas anónimos fuera de línea. En este sistema de dinero electrónico, los comerciantes no necesitan interactuar con los bancos antes de recibir dinero de los usuarios. En lugar de eso, los comerciantes pueden cobrar el dinero gastado por los usuarios y depositar el dinero más tarde en el banco.

1.6.4 Herramientas bancarias

La banca electrónica implica el uso de tecnología de la información. Bajo este sistema de tecnología de la información, los servicios bancarios se entregan a través de un sistema controlado por computadora. Este sistema utiliza una interfaz directa con los clientes, es decir los clientes no tienen que visitar las instalaciones del banco.

Entre las principales ventajas de la banca electrónica se encuentran las siguientes:

- El costo operativo por unidad de servicios es menor para los bancos.
- Ofrece comodidad a los clientes ya que no están obligados a ir a las instalaciones del banco.
- Hay muy baja incidencia de errores.
- El cliente puede obtener fondos en cualquier momento de cajeros automáticos.
- Las tarjetas de crédito y débito permiten a los clientes obtener descuentos en puntos de venta.
- El cliente puede transferir fácilmente los fondos de un lugar a otro electrónicamente.

Entre los servicios que ofrece la banca electrónica se cuentan: los cajeros automáticos, “las tarjetas de crédito, tarjetas de débito, sistema de transferencia electrónica de fondos,

banca móvil, banca por Internet, telebanca y sistema de pago de truncamiento de cheques" (Amarasiri & Dias, 2015).

Debido a los servicios que ofrecen, las entidades bancarias deben innovar los sistemas informáticos para que los usuarios puedan realizar sus transacciones virtualmente como lo señala el informe de la OEA:

> *"Los usuarios privilegian los medios virtuales sobre los presenciales, lo cual concuerda con el alto grado de digitalización de los servicios y el impulso a la utilización de éstos, ya que el 53% de los encuestados revisa transacciones y saldos usando teléfonos inteligentes más que los que consultan en el banco (29%) o por línea telefónica (23%), e igualmente prefieren transferir fondos a través de Banca Móvil (43%) que trasladándose al banco (37%)"* (Organización de los Estados Americanos, 2018).

En Ecuador existen soluciones enfocadas a la disponibilidad del usuario como la banca móvil ofrecida por entidades financieras tales como: Banco Pichincha, Banco Pacífico, Produbanco, etc. Adicionalmente, existe software ofrecido por empresas como TATA que se enfocan en Bitcoins Quartz Blockchain Solutions (Tata Consultancy Services, 2019). Por su parte, CobisCorp ofrece herramientas enfocadas en préstamos, garantías, cartera, cuentas, depósitos, tesorería, servicios bancarios y comercio exterior (COBIS Financial Agility Partners, 2015).

La disponibilidad con la que funcionan las transferencias bancarias, por ejemplo en Produbanco, permiten a las personas que no poseen cuentas bancarias retirar dinero de los cajeros por medio de un código que se envía al usuario por celular. Otro ejemplo es BIMO, Billetera móvil, que pide como requisitos: cédula de identidad y una cuenta bancaria en cualquiera agencia que pertenezca a BANRED.

1.6.5 Legislación vigente en Ecuador

El producto de software dinero electrónico es una abstracción financiera que requiere ser regulada por organismos estatales tales como: Banco Central del Ecuador y Contraloría General del Estado. Todos los recursos de información deben cumplir con las leyes dictaminadas conforme a la jurisdicción de cada país, las leyes de software bancario en Ecuador y artículos más relevantes para el caso de estudio son las siguientes:

- Constitución de La República del Ecuador 2008.
- Código Orgánico Monetario y Financiero (COMF).
- Ley Orgánica para la Reactivación de la Economía, Fortalecimiento de la Dolarización y Modernización de la Gestión Financiera.

En consonancia, se cita los artículos con los que debería cumplir el sistema:

El artículo 302, de la "Constitución de la República del Ecuador publicada el 20 de octubre del 2008, en su Título VI Régimen de Desarrollo, Capítulo Cuarto, Sección Sexta de Política Monetaria, señala: que uno de los objetivos que tendrán las políticas monetarias, crediticia y cambiaria y financiera, consiste en *Establecer niveles de liquidez global que garanticen adecuados márgenes de seguridad financiera"* (Constitución de la República del Ecuador, 2008).

El artículo 309, de la misma ley establece: *"El sistema financiero nacional se compone de los sectores público, privado, y del popular y solidario, que intermedian recursos del público. Cada uno de estos sectores contará con normas y entidades de control específicas y diferenciadas, que se encargarán de preservar su seguridad"* (Constitución de la República del Ecuador, 2008). *Por lo que se debe respaldar "la seguridad en software bancario revisando en su ciclo de vida cumpliendo con los requerimientos y aplicando Criptografía"* (Constitución de la República del Ecuador, 2008).

El Capítulo 2, de la COMF, en su sección 1, artículo 14, señala que la Junta de Política y Regulación Monetaria y Financiera tiene entre sus funciones *"Regular la gestión de los medios de pago electrónicos operados por las entidades del sistema financiero nacional*". Del análisis del el artículo citado se desprende que existe la posibilidad de que cualquier entidad financiera, cuyo funcionamiento sea legal, puede utilizar un sistema de dinero electrónico. Esta apertura plantea la necesidad de que se homologue las normativas, a través del consecuente diseño de un prototipo basando en estándares internacionales.

El mismo cuerpo normativo, en su título II, capítulo I, sección 4, artículo 152, relativo a los derechos de las personas, refiere que *"las personas naturales y jurídicas tienen derecho a disponer de servicios financieros de adecuada calidad, así como a una información precisa y no engañosa sobre su contenido y características*" (Código Orgánico Monetario y Financiero, 2014).

Por su parte, el artículo 155, de la mencionada ley, relacionado con la protección, señala: "*en los términos dispuestos por la Constitución de la República, este Código y la ley, los usuarios financieros tienen derecho a que su información personal sea protegida y se guarde confidencialidad"* (Código Orgánico Monetario y Financiero, 2014).

Por otro lado, los Artículos 152 y 155 justifican la confidencialidad e integridad para los usuarios, características requeridas por el sistema a diseñarse.

El artículo 101, del COMF, sobre medios de pago electrónicos, indica: *"los medios de pago electrónicos serán implementados y operados por las entidades del sistema financiero nacional de conformidad con la autorización que le otorgue el respectivo organismo de control"* (Código Orgánico Monetario y Financiero, 2014).

"Todas las transacciones realizadas con medios de pago electrónicos se liquidarán y de ser el caso compensarán en el Banco Central del Ecuador de conformidad con los procedimientos que establezca la Junta de Política y Regulación Monetaria y Financiera" (Código Orgánico Monetario y Financiero, 2014).

"Para efectos de supervisión y control en el ámbito de sus competencias, los organismos de control respectivos y el Banco Central del Ecuador, mantendrán interconexión permanente a las plataformas de las entidades del sistema financiero a través de las cuales se gestionen medios de pago" (Código Orgánico Monetario y Financiero, 2014). La Ley Orgánica para la Reactivación de la Economía, Fortalecimiento de la Dolarización y Modernización de la Gestión Financiera señala en sus artículos relevantes de dinero electrónico, las siguientes modificaciones:

- Sustituir el numeral 21 del Artículo 14 del Código Orgánico Monetario y Financiero por el siguiente: *"regular la gestión de los medios de pago electrónicos operados por las entidades del sistema financiero nacional, y disponer al Banco Central del Ecuador su control, monitoreo y evaluación; así como de la moneda nacional metálica, de acuerdo con lo dispuesto en este Código"* (Código Orgánico Monetario y Financiero, 2014).
- Efectuar la siguiente reforma al artículo 36 del COMF: en el numeral 2, antes del punto final, inclúyase la frase: "*y realizar el control de las transacciones en medios de pago electrónicos que se realicen a través de las plataformas del sistema financiero nacional con fines de supervisión monetaria, para lo cual las entidades financieras brindarán acceso permanente y sin restricciones a dichas plataformas"* (Código Orgánico Monetario y Financiero, 2014).

1.6.6 ISO 27001

ISO / IEC 27001 es uno de los estándares más populares del mundo, orientada en la protección de la información de una empresa. La norma ISO 27001 "es una solución de mejora continua en base a la cual puede desarrollarse un Sistema de Gestión de Seguridad de la Información (SGSI) que permita evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización tanto propia como datos de

terceros. Por otro lado, también permite establecer los controles y estrategias más adecuadas para eliminar o minimizar dichos peligros" (ISO/IEC 27001, 2013).

ISO / IEC 27001: 2013 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. "También incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en ISO / IEC 27001: 2013 son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza" (ISO/IEC 27001, 2013) .

1.6.7 COBIT

El marco COBIT proporciona una gran cantidad de información para que la empresa logre sus objetivos, a través de la gestión de los recursos de TI basados en el proceso de agrupación. COBIT fue creado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA) y el Instituto de Gobierno de TI (ITGI) en 1992. COBIT ha sido publicado cuatro veces. La primera versión se publicó en 1996. Le siguen en 1998, 2000 y la cuarta en 2005. La quinta versión se lanzaro en 2012.

La base del marco COBIT es proporcionar una política clara y buenas prácticas en el gobierno de TI. Su objetivo es ayudar a la gerencia, al auditor y al usuario a comprender y administrar los riesgos asociados con el gobierno de TI al ofrecer un conjunto de procesos estructurados para presentar la información necesaria, a fin de cerrar la brecha entre los riesgos comerciales, las necesidades de control y los problemas técnicos.

Para el aspecto de gestión, COBIT proporciona una dirección clara en términos de proporcionar los valores de "CSF (Factores críticos de éxito), KGI (Indicadores clave de objetivos), KPI (Indicadores clave de rendimiento) y Modelo de madurez (0; inexistente, 1; inicial / ad -hoc, 2; repetible pero intuitivo, 3; proceso definido, 4; administrado y medible, y 5; optimizado)". (Haviluddin & Anthony, 2012)

1.6.8 NISTIR 7977

Las normas y pautas criptográficas para la protección de los sistemas de información siempre han sido un componente clave de la NIST. Para llevar a cabo su misión de proteger la información y los sistemas de información, NIST también debe participar activamente en el avance del campo de la criptografía. NIST se compromete a lograr estos objetivos

garantizando que sus capacidades internas sean sólidas y efectivas, y que tenga acceso a criptógrafos externos altamente capaces.

NIST cree que los procesos de desarrollo robustos, ampliamente entendidos y participativos producen los estándares y lineamientos criptográficos más sólidos, efectivos, confiables y ampliamente aceptados. Los siguientes principios guían los procesos de desarrollo de pautas y estándares criptográficos del NIST.

Transparencia: todas las partes interesadas y afectadas tienen acceso a información esencial sobre las normas y actividades relacionadas con las directrices durante todo el proceso de desarrollo.

Apertura: la participación está abierta a todas las partes interesadas.

Equilibrio: NIST se esfuerza por lograr un equilibrio de intereses entre las partes interesadas, sopesando estos intereses para desarrollar estándares y pautas criptográficas que sean seguros y eficientes, y que promuevan la interoperabilidad. (NIST, 2016)

Integridad: NIST sirve como una autoridad técnica imparcial cuando desarrolla estándares y pautas criptográficas.

Como parte del proceso de desarrollo de estándares, el NIST evitará o manejará adecuadamente los conflictos de intereses, siguiendo los procedimientos para manejar el riesgo presentado por esos conflictos y garantizará la capacitación adecuada para su personal. (NIST, 2016)

2. METODOLOGÍA

La Metodología de diseño se adapta para cumplir lo que se ha planteado cómo características y requerimientos del proyecto para un sistema determinado. El papel de la metodología de diseño de software no puede exagerarse (Freeman, The nature of design, 1980). Esta proporciona un medio lógico y sistemático para continuar con el proceso de diseño, así como un conjunto de pautas para la toma de decisiones. Además, realiza una secuencia de actividades y, a menudo, utiliza un conjunto de notaciones o diagramas.

La metodología de diseño es especialmente importante para proyectos grandes y complejos que involucran programación en grande (donde participan muchos diseñadores). El uso de una metodología establece un conjunto de canales de comunicación comunes para traducir el diseño a códigos y un conjunto de objetivos comunes. Adicionalmente, para que una metodología sea eficiente, debe haber una

coincidencia objetiva entre el carácter general del problema y las características del enfoque de solución(Freeman & Wasserman, 1980).

2.1. Explicación de la metodología

La metodología de diseño presenta perspectivas distintas para su realización, de las cuales se ha seleccionado dos para el presente proyecto. La primera fue elaborada por Isaac Asimov, quien ideó siete fases con estructura lineal y cronológica que permiten diseñar los proyectos. Estas fases están divididas en dos grupos principales. Las primeras tres, agrupadas en fase de diseño, son: el diseño buscando la factibilidad, primer prototipo y detalle del mismo. Los cuatro restantes, agrupadas en el ciclo de fases de producción y consumo, son: planeación de construcción, planeación de distribución, planeación de consumo y planeación del retiro.

Por el alcance del presente proyecto se considera la implementación hasta la cuarta fase, relacionada a la construcción del proyecto. Las fases restantes no serán consideradas debido que no se realizará la implementación del sistema.

Sin embargo, es preciso considerar que Asimov propuso una metodología que contempla inclusive el momento que el software concluye su ciclo de vida, con el retiro del sistema. Esta metodología se detalla en la Ilustración 1.

La segunda perspectiva, de Nigel Cross, presenta un modelo en ocho etapas, cuya principal función consiste en dividir el problema en varios subproblemas. Las referidas etapas se agrupan en dos conjuntos. El primero incluye objetivos, funciones, requerimientos y características; mientras que el segundo comprende oportunidades, mejoramiento, evaluación y alternativas, como mecanismos de retroalimentación de las primeras. Esta segunda perspectiva se presenta a detalle en la ilustración 2.

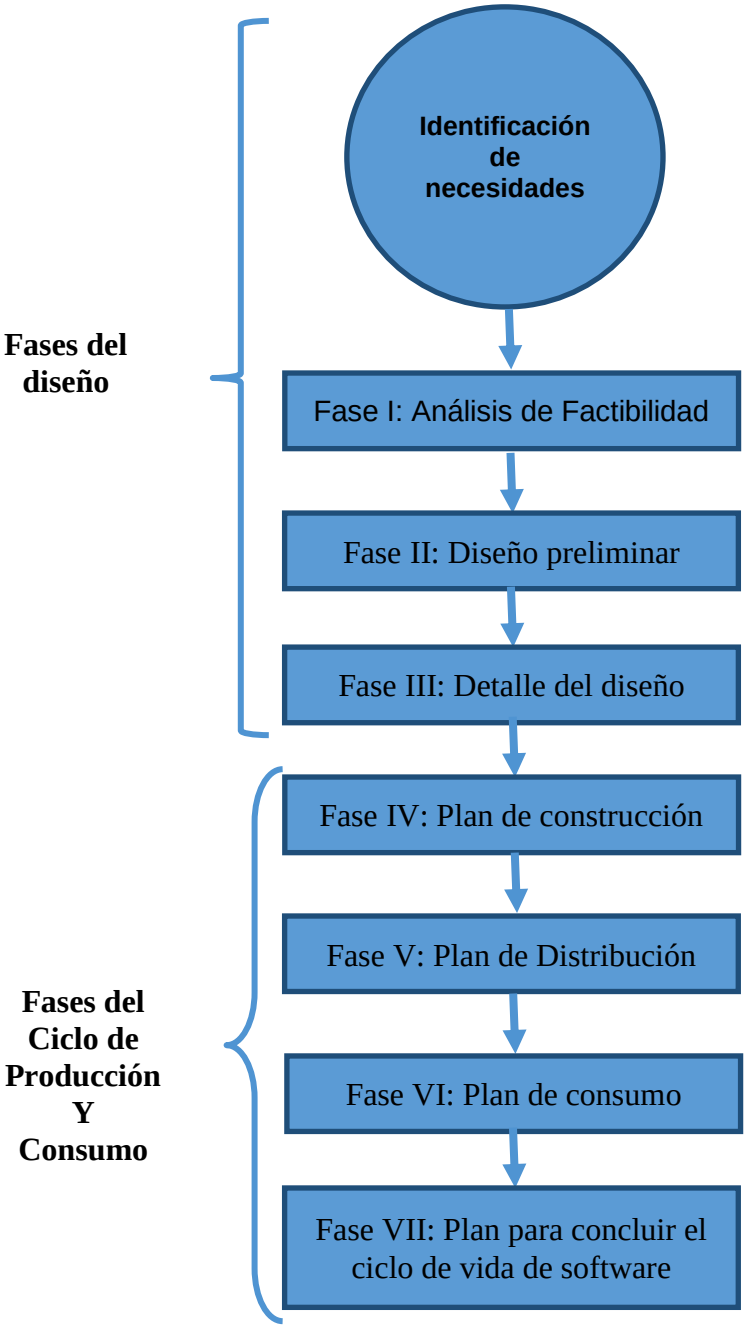


Ilustración 1: metodología del diseño Morris Asimov
Fuente: **(Asimov, 1962)**

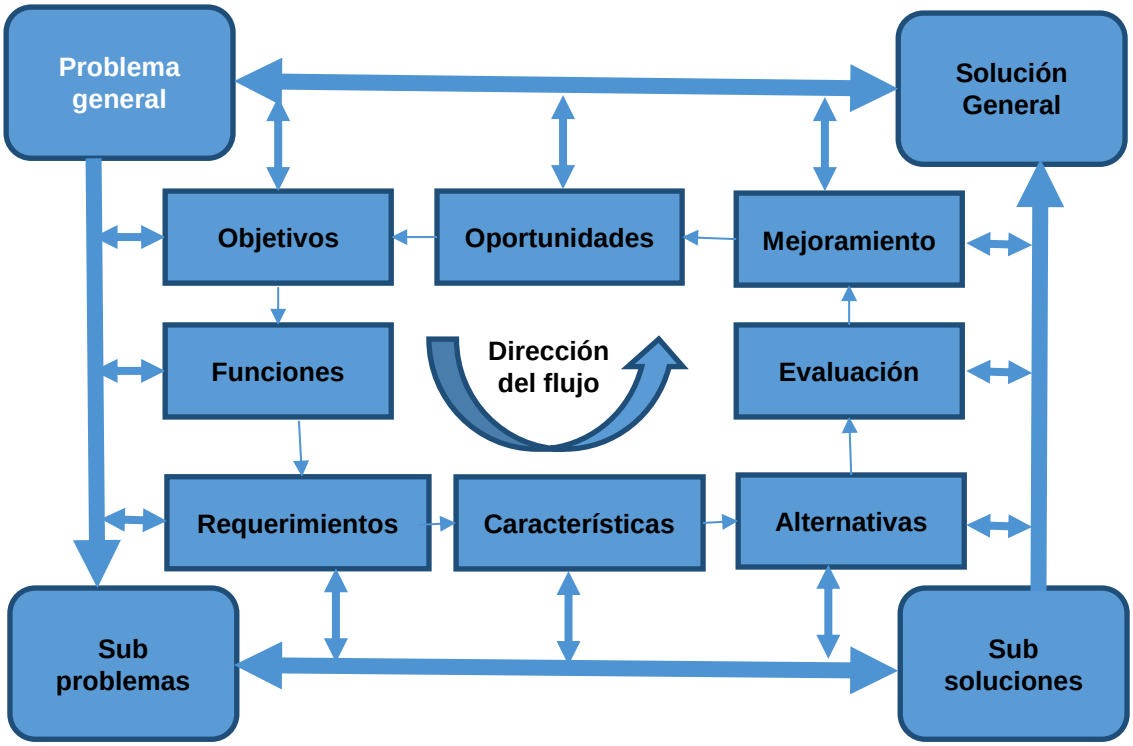


Ilustración 2: metodología diseño Nigel Cross
Fuente: **(Cross, 2008)**

2.1.1. Características de la Metodología de Diseño

Adams propone la aplicación de ciertas características para el desarrollo de la metodología, mismas que se han contrastado en el desarrollo del proyecto, arrojando los resultados presentados en la **¡Error! No se encuentra el origen de la referencia.** (Adams, 2015):

Tabla 1: aplicación metodología del diseño

Característica	Definición	Aplicación
Exploratoria	El diseño requiere conocimientos específicos, destrezas y habilidades.	El diseño de un sistema bancario requiere conocimiento de las leyes que deben aplicarse y conocimiento en las herramientas a utilizarse.
Racional	El diseño involucra razonamiento lógico, análisis matemático, simulación por ordenador, experimentación, etc.	El diseño de un sistema criptográficamente seguro involucra análisis matemático exhaustivo y requiere pruebas y simulación.

Característica	Definición	Aplicación
Investigación	Investigar requisitos de las partes interesadas, soluciones de diseño anteriores. Fallos y éxitos de diseño, etc.	En Ecuador hubo un sistema billetera móvil **EFECTIVO** del Banco Central del Ecuador.
Creatividad	El diseño requiere conocimientos técnicos, reconocimiento de patrones, pensamiento lateral, lluvia de ideas, analogías, etc.	El diseño requiere conocimientos técnicos actualizados constantemente tomando en cuenta que las amenazas a sistemas bancarios crecen exponencialmente a diario.
Oportunidad	Analizar los problemas que se van presentando en cada etapa del ciclo de vida del software y ofrecer soluciones.	Por el alcance del proyecto se presentará un prototipo, pero se debe dejar un precedente para trabajos futuros.
Incremental	A los requisitos que se presentan durante el proceso para mejorar el sistema y que se adapten al diseño.	El diseño de este proyecto puede variar sus requisitos por cada entidad bancaria.
Toma de decisiones	Soluciones que requieren juicios de valor dadas por las partes interesadas del sistema analizando la competencia.	El prototipo del proyecto debe contrarrestar las necesidades de los clientes y la legislativa en el Ecuador.
Iterativo	Los artefactos entregados son analizados basándose en requerimientos funcionales y no funcionales abiertos a la retroalimentación por parte del usuario.	El proyecto puede presentar variaciones cuando el usuario lo pruebe por lo cual debe ser abierto a modificaciones y mejoras constantes.
Transdiciplinario	Un equipo transdisciplinario no sólo técnico.	En el proyecto se involucra el sector financiero, el sector legislativo y los usuarios finales.
Interactivo	Equipo de diseño es una parte integral.	El equipo del presente proyecto conformado por el director, desarrollador y cliente.

Elaborado por: Mónica Vargas, 2020.

2.2. Análisis de las metodologías de desarrollo de software

Algunos proyectos de desarrollo de software incurren en errores de diseño provocando extensiones en tiempo y costo. Los errores más expansivos a menudo se introducen temprano en el proceso de desarrollo. Esto subraya la necesidad de una mejor definición de requisitos y metodología de diseño de software (Asimov, 1962).

El diseño de software es una actividad importante, ya que determina cómo procedería toda la tarea de desarrollo de software, incluyendo el mantenimiento del sistema. El diseño del software es esencialmente una habilidad, pero generalmente requiere una estructura que proporcionará una guía o una metodología para esta tarea.

Una metodología puede definirse como los principios y reglas subyacentes que rigen un sistema. Un método puede definirse como un procedimiento sistemático para un conjunto de actividades. Por lo tanto, a partir de estas definiciones, una metodología completa abarcará los métodos utilizados dentro de la metodología. Diferentes metodologías pueden apoyar el trabajo en diferentes fases del ciclo de vida del sistema. Es por eso que a continuación se hace un resumen de las metodologías de diseño más usadas para el desarrollo de software.

Tabla 2: Metodologías de desarrollo de software

Metodología	Definición	Pros	Contras
Modelo de cascada	Es considerado como el método tradicional para explicar el proceso de desarrollo de software en la ingeniería de software, el modelo en cascada aclara el proceso en un flujo lineal con una secuencia específica para que los usuarios entiendan que el nivel adicional se hace progresivo al completar el anterior. Además, esta metodología también habla del hecho de que no es posible volver a lidiar con los cambios.	Fácil de entender y funcional. Suficientemente simple de manejar ya que el modelo es rígido Ahorra mucho tiempo Permite pruebas y análisis fáciles	Solo coincide con necesidades precisas No aplica para proyectos de mantenimiento. No hay opción para conocer el posible resultado de un proyecto. No es excelente para proyectos largos y en curso.
Metodología del prototipo	Es un procedimiento de desarrollo de software especializado que inicia a los desarrolladores a hacer solo la muestra de la resolución para validar su esencia funcional a los clientes y realizar cambios esenciales antes de crear la solución final auténtica. De hecho, la mejor parte de esta metodología es que tiende a resolver un conjunto de problemas de diversificación que ocurren con el método de cascada.	Da una idea clara sobre el proceso funcional del software. Reduce el riesgo de falla en la funcionalidad de un software Ayuda bien en la recopilación de requisitos y el análisis general	Posibilidades de extensión en el costo de gestión La participación excesiva del cliente puede afectar el procesamiento Demasiados cambios afectan el flujo de trabajo del software

Metodología	Definición	Pros	Contras
Metodología de desarrollo ágil	Como enfoque innovador, la metodología de desarrollo de software ágil se utiliza para articular un procedimiento de gestión de proyectos bien organizado que permita alteraciones recurrentes. Ciertamente, este tipo de metodología es un esbozo teórico para emprender varios proyectos de ingeniería de software. Otra cosa buena es que minimiza el peligro al crear software en cuadros de tiempo cortos, conocidos como iteraciones, que duran de una semana a un mes.	Enfoque adaptativo que responde favorablemente a los cambios. Permite la comunicación directa para mantener la transparencia. Mejora de la calidad al encontrar y corregir defectos rápidamente e identificar temprano los desajustes de expectativas.	Se enfoca en trabajar con software y carece de eficiencia de documentación Las posibilidades de salirse del camino como resultado no están claras
Desarrollo rápido	Con el objetivo de proporcionar resultados rápidos, el desarrollo rápido de aplicaciones está destinado a proporcionar excelentes procesos de desarrollo con la ayuda de otros enfoques de desarrollo. Está creado para aprovechar al máximo el software de desarrollo. Sin lugar a dudas, está diseñado para aumentar la viabilidad de todo el procedimiento de desarrollo de software para resaltar la participación de un usuario activo.	Hace que todo el proceso de desarrollo sea sencillo Ayuda al cliente a tomar revisiones rápidas Fomenta los comentarios de los clientes para mejorar	Depende del equipo para el rendimiento Funciona en un sistema modularizado limitado a esta metodología. Requiere personal extremadamente calificado para manejar complejidades No aplica para proyectos pequeños presupuestados
Metodología del modelo de desarrollo dinámico	Auténticamente formulado y derivado de la metodología de desarrollo rápido, es un enfoque iterativo e incremental que se enfoca en la participación del usuario. La tarea de esta metodología es proporcionar sistemas de desarrollo de software dentro del marco de tiempo especificado y el presupuesto asignado. La razón por la cual es bastante demandada en el mundo del desarrollo de software.	Los usuarios obtienen un control del proceso de desarrollo de software. Los entregables de funcionalidad son rápidos Ofrece fácil acceso a los usuarios finales por parte de los desarrolladores.	Esta metodología es costosa de implementar No apto para organizaciones pequeñas.

Metodología	Definición	Pros	Contras
Metodología de programación extrema	Se identifica por el hecho de que la participación del cliente en el proceso de desarrollo de software es increíblemente alta. Como metodología ágil de ingeniería de software, la metodología de programación extrema se conoce actualmente como metodología XP. Se utiliza principalmente para crear software dentro de una atmósfera muy desequilibrada. Permite una mayor trazabilidad dentro del procedimiento de modelado. El objetivo principal de este modelo XP es reducir el costo de las funcionalidades del software. Es bastante mutuo en el modelo XP que el precio de alterar los requisitos en una etapa futura del proyecto puede ser realmente sorprendente.	Se centra en la participación del cliente. Establece planes y horarios racionales. Los desarrolladores están excepcionalmente comprometidos con el proyecto. Equipado con métodos modernistas para software de calidad.	La efectividad depende de las personas involucradas Requiere reunión frecuente para el desarrollo aumentando los costos totales Necesidades para cambios de desarrollo excesivos Las posibilidades exactas y los resultados futuros son realmente desconocidos
Metodología de desarrollo de Scrum	El modelo de desarrollo de Scrum Software se inicia con una planificación efímera, una conferencia y se completa con una revisión final. Esta metodología de crecimiento se usa para el desarrollo rápido de software que incluye una serie de iteraciones para generar el software requerido. Es un enfoque perfecto porque sin esfuerzo pone en marcha los proyectos progresivos deliberados.	La toma de decisiones está en manos del equipo. El documento de requisitos comerciales se considera insignificante Método ligeramente controlado que simpatiza con la actualización constante	El método de procesamiento sufre debido a los costos vacilantes No apto para proyectos de gran tamaño. Requiere un equipo altamente experto, que no tiene lugar para principiantes

Fuente: (Atwood, Ramsey, & Campbell, 2015)

2.3. Aplicación de la metodología de diseño

2.3.1. Fase I: Análisis de Factibilidad

El proyecto ha analizado la forma de funcionamiento de dos sistemas operativos en el "Banco Central del Ecuador: Sistema de Pagos Interbancario (**SPI)** y **EFECTIVO** de dinero electrónico, del Banco Central del Ecuador; el cuál funcionaba de la siguiente forma" (Banco Central del Ecuador, 2016):

a. Activación de cuenta de dinero electrónico por medio del dispositivo móvil.

b. Compra de dinero en el Banco Central del Ecuador.
c. Pagos y transferencias a entidades con cuentas de **EFECTIVO**.

Lo cual indica que se realizan transacciones de incremento y débito de saldo, mismas que son consideradas las principales funciones que cumplía el software **EFECTIVO**.

2.3.2. Levantamiento de Requerimientos

Se debe tomar en cuenta que para este prototipo, el banco ya cuenta previamente con sus propios sistemas de dinero electrónico y el registro de los usuarios tanto como la autentificación, y las transacciones provienen de estos sistemas. El prototipo como tal, busca solucionar, sin invadir la privacidad de los servidores o sistemas bancarios ya existentes en las entidades, la interconexión y reportarla hacia la Entidad reguladora, que en el caso de Ecuador es el Banco Central.

Luego de haber estudiado las normativas generales, dictadas por la Superintendencia de Bancos, se ha tomado para este primer prototipo los siguientes requerimientos básicos:

Tabla 3: requerimiento identificar entidad bancaria

R-001 Identificar Entidad Bancaria	
Característica de Software	Registro de entidades bancarias y confidencialidad de datos
Dependencias	• Identificar usuario posea cuenta bancaria • Identificar usuarios que no posean cuenta bancaria
Precondiciones	El banco valida la información de sus usuarios por medio de sus sistemas
Descripción	El sistema debe reconocer, almacenar datos mínimos del usuario y de la transacción a realizarse.
Secuencia normal	1. Obtención de información del usuario o cliente banco 2. Obtención de información de la transacción
Post Condición	Se procede con la certificación
Excepción	La información recibida del banco sea incompleta
Comentarios	Involucrar a personas que no poseen cuentas bancarias Facilitar la entrega de reportes sobre transacciones a la Entidad reguladora

Fuente: Mónica Vargas, 2020

Con los insumos de la tabla 3, se realiza la siguiente tabla.

Tabla 4: requerimiento generación certificado

R-002 Generación de certificados	
Característica de Software	Autentificación de transacción
Dependencias	La transacción ingresa en un proceso de revisión para cumplimiento de normativas establecidas por la entidad reguladora y la entidad bancaria

	Identificar que la entidad bancaria está autorizada para generar Certificados de Autentificación
Precondiciones	• Las entidades bancarias deben contar con el servidor que respalde cada una de las acciones • La entidad bancaria debe contar con una unidad que genere Certificados de Autentificación
Descripción	El sistema de la entidad bancaria crea el Certificado de Autentificación y la entidad reguladora por medio de su sistema comprueba la validez de los Certificados de Autentificación creados.
Secuencia normal	1. Certificado de autentificación generado 2. Revisión de que se encuentra el Certificado de Autentificación es correcto.
Post Condición	Se procede al almacenamiento y replicación de la transacción
Excepción	Alguna de las entidades bancarias no genere el certificado de autentificación o sea generado incorrectamente
Comentarios	

Fuente: Mónica Vargas, 2020

Tabla 5: requerimiento almacenamiento y replicación de transacción

R-003 Almacenamiento y replicación de transacción	
Característica de Software	No repudio
Dependencias	La interconexión a los servidores de almacenamiento
Precondiciones	• La transacción ha cumplido con todas las normativas establecidas • La transacción cuenta con Certificados de Autentificación aprobados
Descripción	El sistema almacena la transacción aprobada y replica a cada uno de los nodos.
Secuencia normal	1. La transacción aprobada es almacenada en el servidor 2. La transacción almacenada es adherida al blockchain 3. El blockchain de transacciones es actualizado en cada uno de los nodos
Post Condición	
Excepción	Las transacciones rechazadas no son adheridas al blockchain ni replicadas ya sea por qué alguna de las dos entidades bancarias no han aceptado la transacción o en su defecto no ha cumplido con alguna de las normativas
Comentarios	Reducir el anonimato para evitar lavado de activos e incluso incluir a personas que no poseen cuentas bancarias

Fuente: Mónica Vargas, 2020.

2.4. Métodos y Herramientas de Trabajo

Se ha determinado utilizar la entrevista cómo recurso para el levantamiento de requerimientos dado que el proyecto es de carácter general y puesto que no se empleará una entidad bancaria específica. La encuesta es cualitativa, lo que permite realizar una tabla de requerimientos. Se ha determinado utilizar el Framework Hyperledger Fabric en función de los objetivos planteados en este proyecto.

2.4.1. Normas Seguridad

Las normas utilizadas en los sistemas del Banco Central del Ecuador son legislativas, mismas que se resaltan en cada uno de los manuales y son las siguientes (Banco Central del Ecuador, 2011):

- Constitución de la República del Ecuador
- Ley de Régimen Monetario y Banco del Estado
- Ley de Comercio Electrónico y su Reglamento
- Codificación de Regulaciones del Banco Central del Ecuador

No se destaca ninguna normativa de tipo seguridad informática adicional a la nomartiva legal con la que se maneja el sistema. Tampoco se establece alguna normativa propia o aplicada tanto en el informe realizado por auditoría Informática donde se analizó el Sistema de Pagos Interbancario, como en los manuales de este mismo sistema realizados por el Banco Central del Ecuador.

En la Tabla 6 se especifican las ventajas y desventajas de normas de seguridad, por medio de sus aplicaciones, para elegir la que mejor se adapte al prototipo a presentarse.

Tabla 6: comparación normas

Norma	Costos	Tamaño Empresa	Etapa de ciclo de vida de Software	Documentación	Innovación
OCTAVE	Alto	Grande	Producción	Alto	Medio
MARGERIT	Medio	Mediana Grande	Producción	Bajo	Bajo
ISO27000	Bajo	Mediana Grande	Producción	Medio	Medio
ISO 9000	Bajo	Mediana Grande	Producción	Medio	Medio
NIST	Bajo	Mediana Grande	Diseño	Alto	Alto

Fuente: Mónica Vargas, 2020.

Con base en los parámetros de la tabla comparativa, se considera que NIST es la norma que mejor se adapta al ambiente planteado, debido a que se puede implementar durante las etapas de desarrollo; de esta forma se tiene acceso libre a documentación que facilita la adaptación a los requerimientos.

2.4.2. NIST

Este proyecto se basa en encriptación por lo cual se tomó como referencia la aplicación de estándares de criptografía y la Guía de Procesos de Desarrollo (*NISTIR 7977)*.

Las normas NIST se encuentran ubicadas por debajo de cualquier norma que se aplique en cada país, motivo por el cual se analizó previamente las normas ecuatorianas en la normativa vigente en Ecuador para llevar a cabo este proyecto. La actualización de esta guía va a ser realizada mediante NIST y las organizaciones que se considere prudentes.

Los principios que NIST considera necesarios para realizar procesos de desarrollo y estándares de criptografía robustos son los siguientes (NIST, 2016):

a. Transparencia: se refiere a la información esencial de cada proyecto y a su documentación. Este principio se cumple cuando las partes interesadas poseen acceso a la información generada. En este sentido, Hyperledger Fabric cuenta con manuales y código abierto.
b. Apertura: fomenta la participación de usuarios, investigadores, profesionales en seguridad tienen una oportunidad de participar en el proceso de desarrollo de normas y directrices. Al respecto, Hyperledger Fabric permite descargar los proyectos, modificarlos, y subirlos para toda la comunidad.
c. Balance: promueve el equilibrio entre las partes interesadas, ya sean el gobierno, la industria o la academia; para desarrollar directrices, normas criptográficas eficaces y seguras. A tal efecto, Hyperledger Fabric fue diseñado para la industria, y se puede realizar e implementar siguiendo normativas gubernamentales.
d. Integridad: se reconocerá el trabajo realizado, sin tergiversarlo, siendo una autoridad técnica imparcial.
e. Mérito técnico: toma decisiones durante el desarrollo de estándares criptográficos y directrices basando sus elecciones por mérito técnico de cada propuesta; teniendo en cuenta la seguridad, privacidad, política y consideraciones comerciales. Se esfuerza por estandarizar criptografía segura, algoritmos, esquemas y modos de operación cuyas propiedades de seguridad sean robustas.
f. Aceptación Mundial: son estándares establecidos para productos y servicios de tecnología de la información desarrollados por Estados Unidos, motivo por el cual buscan la aceptación internacional que permita la protección de sistemas de información.

g. Uso: su objetivo es desarrollar estándares criptográficos y guías que colaboren con los implementadores para la creación de sistemas seguros y utilizables para sus clientes, que puedan adaptarse al futuro.
h. Mejora continua: junto con el desarrollo de algoritmos criptográficos, se promueve en la comunidad criptográfica la identificación de debilidades, vulnerabilidades u otras deficiencias en los algoritmos especificados en las publicaciones.
i. Innovación y propiedad intelectual: debido a la preferencia de los usuarios por soluciones que no se encuentren comprometidas por tecnologías patentadas con derechos de autor. Por lo que, si se adquiere tecnologías con derechos de autor, los costos potenciales sean superados por los beneficios técnicos. Adicionalmente, siempre respetará la propiedad intelectual.

Publicaciones para estándares criptográficos y guías

Las publicaciones se basan en tres niveles específicos:

- Estándares Federales de Procesamiento de la Información.
- Publicaciones Especiales.
- Informes Internos Interinstitucionales (NISTIR).

Stakeholder para los estándares criptográficos

El stakeholder puede ser voluntario para seguir con los estándares. Se propone que tanto empresas de tecnología como usuarios ayuden a la creación de estándares por medio de la publicación de algoritmos creados. Posteriormente, se convoca a voluntariado para realizar y mantener actualizada la información.

Compromiso de la comunidad criptográfica

El reglamento funcionamiento, en consecuencia, con el crecimiento de aportes en la academia y a nivel industrial, es variable. Éste compromete a los usuarios en la aplicación de guías para la criptografía a realizar aportes, siempre invitando a la comunidad a ser partícipe de cada versión. En este sentido, Hyperledger está abierto a colaboraciones, por lo que cumple a cabalidad con este estándar.

Promueve que se compartan los algoritmos de encriptación de tal forma que la comunidad pueda llegar a ellos y realizar las modificaciones pertinentes en caso de tener un fallo de seguridad.

Publicación y revisión de las propuestas y presentación final de estándares y guías

Las publicaciones siempre deben ser transparentes y abiertas a innovación por lo que deben existir manuales, guías, participación, etc. Esto se solicita debido a la necesidad de evaluar transparentemente toda propuesta, y así poder realizar la publicación en documentos finales de estándares o guías.

Políticas y procesos para el manejo de ciclo de vida de los estándares y guías criptográficos

Estas políticas y procesos cubren las primeras etapas del desarrollo y regulan el mantenimiento y revisión

Identificación y evaluación necesaria

Se requiere tomar en cuenta los siguientes aspectos:

- El levantamiento de requerimientos precisa un directivo o administrativo de mayor rango empresarial. Para el proyecto realizado en particular, no se aplica este requerimiento, debido a que es un análisis realizado para empresas bancarias de forma general.
- El desarrollo tecnológico despierta un interés particular, por ejemplo, nuevos avances en tecnología, algoritmos, estándares o guías, exploración de vulnerabilidades, etc.
- Es un área necesaria para el compromiso con la comunidad, al aplicarse los estándares para el desarrollo del proyecto.
- A la comunidad le interesaría este mecanismo o lo consideraría importante, dado que el dinero electrónico es de uso internacional en ciertos países y ya se ha institucionalizado.

Anunciar el proyecto a la comunidad

Considerar el anuncio del proyecto a la comunidad por los distintos medios que se encuentren. De esta forma se recolecta información y comentarios que pueden ser útiles para cada proyecto.

Considerar requerimientos y soluciones

Para los procesos que se llevarán a cabo se requiere

1. Identificación de requerimientos.
2. Investigación de la literatura adecuada.

3. Determinar la opción más apropiada incluyendo el análisis del algoritmo criptográfico.
4. Buscar las pruebas de seguridad para los algoritmos criptográficos o esquemas

Definir un plan específico o un proceso

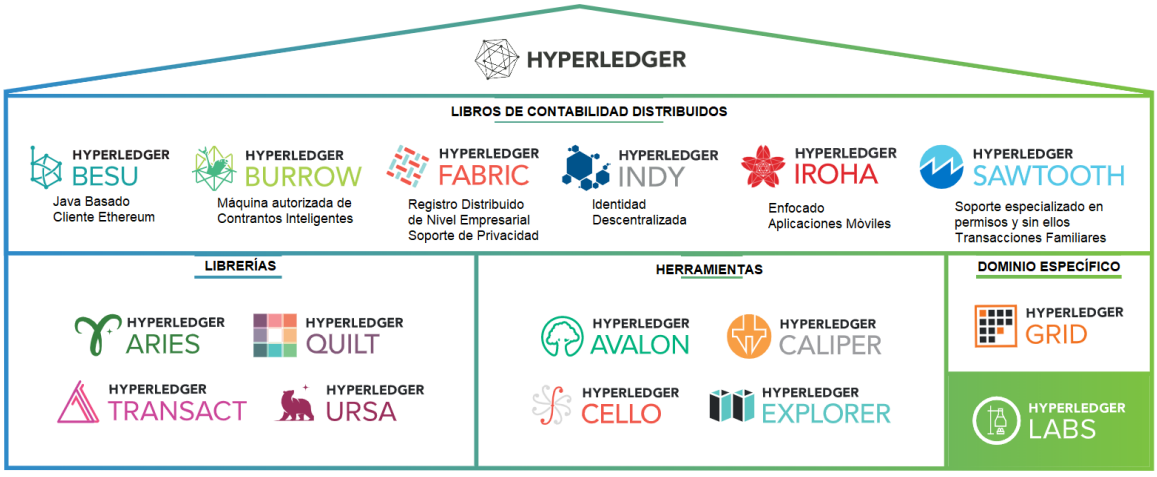
Presentar varios enfoques que se utilizan para satisfacer las necesidades de estándares o pautas criptográficas.

- Trabajar con SDOs propone que acorde a los requerimientos de cada proyecto se trabaje en normas de desarrollo como SDOs. Incluso propone unir esfuerzos por medio de su personal en caso de que sea necesario.
- En caso de no existir un estándar, se requiere desarrollar uno nuevo que debe ser públicamente probado y aceptado para considerarse una contribución significativa.
- Celebrar una nueva competencia cuando se decide realizar una nueva directriz. Se puede hacer mediante una competencia abierta y los competidores pueden ser parte de la industria o academia. En caso de ser reconocidos como ganadores deberán renunciar a los derechos de la directriz para que ésta pueda ser publicada.

2.4.3. Herramientas de Contabilidad

La familia de herramientas de libros de contabilidad distribuidos que ofrece Hyperledger se enfoca en bitcoins, contratos inteligentes identidades, aplicaciones móviles, entre otras. Hyperledger Fabric es la herramienta que se encuentra enfocada en transacciones. Uno de los beneficios notables de la misma es que permite la colaboración de la comunidad con lo que se puede adaptar a la necesidad que se encuentre. En la Ilustración 3 se muestran las diferentes aplicaciones desarrolladas por Hyperledger.

Ilustración 3: herramientas de Hyperledger



Fuente: (IBM, 2016)

2.4.4. Hyperledger Fabric

Hyperledger Fabric es una plataforma que brinda soluciones de contabilidad distribuida respaldada por una arquitectura modular; ofreciendo confidencialidad, flexibilidad y escalabilidad. Admite implementaciones conectables de diferentes componentes, logrando una adaptación a la complejidad de sistemas económicos (IBM, 2016).

2.4.4.1. Aplicación

En la industria farmacéutica, los medicamentos deben pasar por un proceso simultáneo de revisión; por lo que HyperLedger Fabric permite la transferencia de documentación encriptada y una revisión en caso de ser alterada cualquier información un estado de olvido.

En la venta de piezas de aviones retirados Honeywell Aerospace, las transacciones y el inventario de piezas se manejan de forma segura. En ventas de otros productos se realizan ventas y a cada uno de los clientes se les puede ofrecer un precio especial sin que otro cliente se entere del mismo.

Se ha implementado un certificado Hyperledger Fabric (CHFA) que permite realizar transferencias de documentación entre profesionales de distintas áreas de forma confidencial.

2.4.4.2. Conceptos

Libro contabilidad distribuida (distributed ledger): permite realizar varias transacciones de distintos usuarios a la vez, almacenando cada transacción por medio de criptografía y haciendo que cada operación que se realice sea inmutable. Hay un libro general donde se registra cada transacción. Este beneficio podría ser utilizado por el Banco Central y por cada réplica de las transacciones en la entidad bancaria.

Contratos inteligentes (smart contracts): Son los reglamentos que deben regir cada transacción para ser acordada. En nuestro, caso son las tarifas estipuladas por cada entidad bancaria para realizarse la transacción. Cada contrato puede adaptarse al sistema de cada una de las entidades bancarias; es decir, a las tarifas cobradas por transacción. Y cada contrato es controlado por una entidad central, en nuestro caso de aplicación sería el Banco Central del Ecuador.

Concenso (concensus): se realiza una vez que las transacciones que han sido aprobadas son actualizadas en el libro de contabilidad, en el mismo orden que fueron ejecutadas; y

actualizadas en cada una de las copias del libro de contabilidad. Sólo se actualizan las transacciones que son pertinentes para cada entidad bancaria.

Identidad: Consiste en identidad digital encapsulada por medio de un certificado X.509. A cada una de las empresas bancarias se le otorga una identidad por medio de un proveedor de servicios de membresía (MSP). MSP determina además de la identidad de usuario con quien puede interactuar cada usuario en la red realizando transacciones. Para lo cual requiere de PKI y una autoridad de certificación.

Membresías: son ejecutadas por una institución reguladora. En el presente proyecto se propone que sea realizado por el Banco Central del Ecuador, debido a que todas las instituciones bancarias deben ser reguladas por esta institución. En las membresías se determina con quién se realizará las conexiones y bajo que reglamentos o certificados serán admitidos.

2.4.5. Definición de Seguridad

Hyperledger Fabric trabaja con cifrado para comprender su forma de cifrar y la criptografía que utiliza definiremos ciertos términos previos de su funcionamiento.

PKI, infraestructura de clave pública, proporciona comunicaciones de red seguras por medio de los siguientes elementos: clave pública y privada, certificados digitales (Hyperledger Fabric emite X.509), certificados autorizados (CA) y listas de revocación de certificados

Las membresías deben ser realizadas por un proveedor de servicios de membresía. Se comprueba que los CA de raíz e intermedios sean los auténticos y no se encuentren en la lista de revocados. Los CA se pueden manejar por usuario o por organización; su principal diferencia es que usuario maneja un único CA mientras que en las organizaciones son conformados por varios usuarios y varios CA.

Chaincode es un programa realizado en Go, node.js o Java. Es en una interfaz prescrita cuya ejecución se da en un contenedor de Docker aislado de la homologación del proceso de peer. Chaincode es el encargado del Libro de contabilidad inicializa y administra su estado.

2. Diseño

El capítulo contiene el diseño y funcionalidad del prototipo, incluyendo las vulnerabilidades de las cuales se debe proteger a la red y a los servidores una vez que se considere la implementación.

2.1. Diseño del sistema

Para comprender el prototipo, se debe tomar en cuenta como se encuentra organizado Hyperledger Fabric. Este prototipo fue diseñado para comunicarse con otros aplicativos de cada institución bancaria y lo que busca es el aseguramiento de la interconexión entre instituciones bancarias y el Banco Central del Ecuador, siendo la última una entidad reguladora de todos los procesos que se llevan a cabo.

2.1.1. Requerimientos del Sistema

Para inicializar cualquier programa y su instalación de Hyperledger Fabric, se requiere un computador que tenganlos siguientes programas previamente instalados:

a. Sistema operativo por compatibilidad. Se sugiere que se realice con UBUNTU 18.04 LTS.
b. En caso de Windows, instalar previamente CURL.
c. Docker y Docker compose.
d. GO.
e. NodeJS.

Una vez instalado se procede a la clonación del proyecto de Hyperledger Fabric.

2.1.2. Infraestructura de red

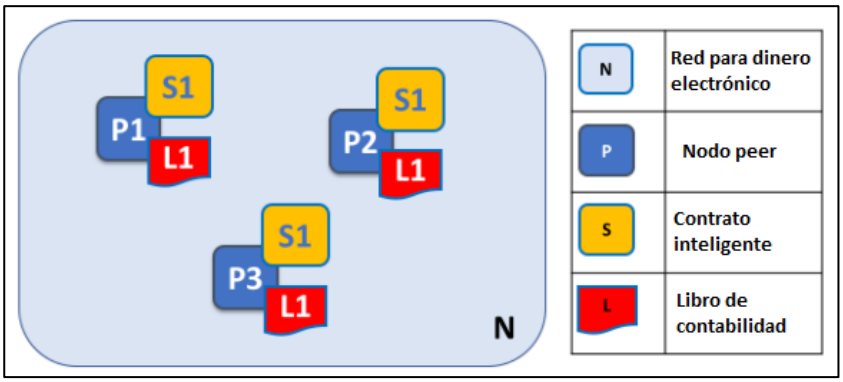
La red inicia con una orden de transacción. En el caso de estudio, esta orden corresponde a un débito o acreditación de un usuario a otro. Primero, se comprueba que el certificado de autentificación sea el correcto, ya que cada certificado de autentificación CA es único para una institución bancaria; sin embargo, puede utilizarse más de uno en cada institución. De esta manera, se tiene un contrato inteligente que cada transacción debe respetar, estos son los cobros o las tarifas con las que se manejan cada institución bancaria y los montos permitidos de transacción por día.

Se debe tener en claro una configuración previa y específica de red hacia donde se va a dirigir cada transacción y las instituciones bancarias con cuales le es permitido

comunicarse, por medio de canales específicos de una institución bancaria a otra. A continuación se explicará punto a punto la construcción de la red y sus elementos.

- Consorcio es la asociación de una o más organizaciones que requieren hacer operaciones entre ellas.
- Canal es el que permite comunicarse a los peers internamente dentro de una red. Existen canales exclusivos creados desde una organización a otra que se utilizan para evitar que la competencia se entere de ciertos privilegios dados a clientes exclusivos. Inclusive estos canales son monitoreados por el administrador de la red. En caso de nuestro proyecto será a través del Banco Central del Ecuador.
- Peer son los nodos iguales que componen una red de blockchain. En cada nodo se alberga un libro de contabilidad y un contrato inteligente. En el caso de estudio cada nodo pertenecerá a una institución bancaria

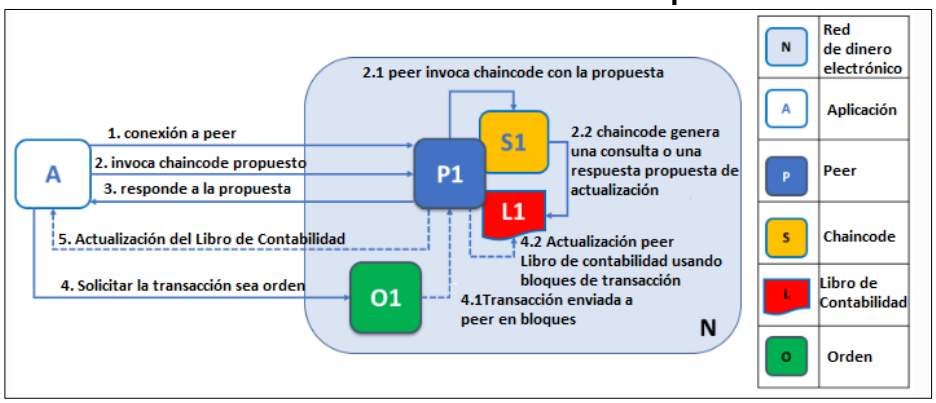
Ilustración 4: funcionamiento de Red



Fuente: (IBM, 2016)

Los nodos peers son los encargados de que cada una de las transacciones se realice de forma múltiple en el mismo servidor. Para comprender lo que realiza el peer y cada una de las acciones consecuentes, se puede observar la Ilustración 5 con cada una de las acciones ejecutadas por cada peer al momento de que el banco solicita una transacción. En la infraestructura de aplicación se especificará el funcionamiento de las transacciones con mayor detalle.

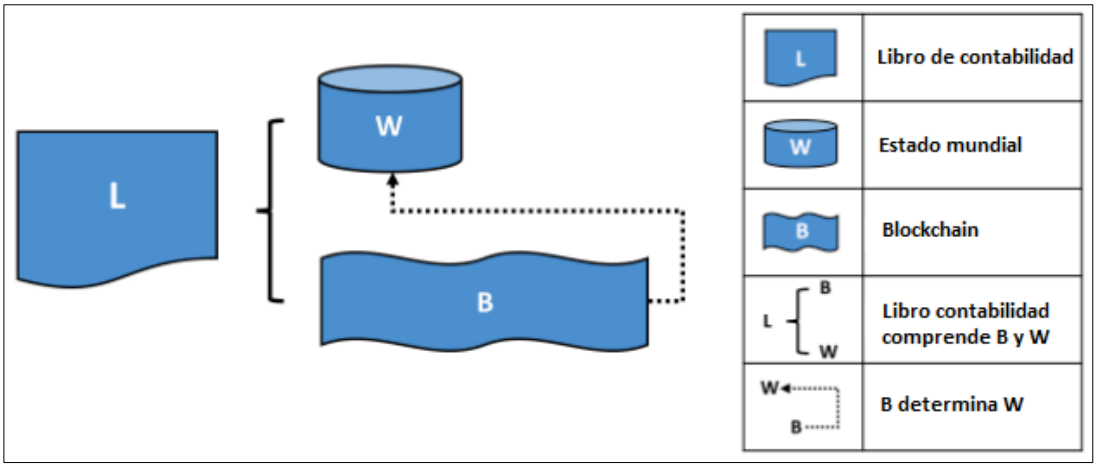
Ilustración 5: funcionamiento del peer



Fuente: (IBM, 2016)

- Libro de contabilidad: consta de dos partes principales: una base de datos del estado mundial que contiene valores actuales por medio de pares clave – valor; estos pares son variables que se pueden crear, actualizar o eliminar; y blockchain que es un registro de todas las transacciones que resultan en el estado actual mundial, está estructura es diferente del estado mundial por qué es inmutable una vez escrita.

Ilustración 6: funcionamiento Libro de Contabilidad



Fuente: (IBM, 2016)

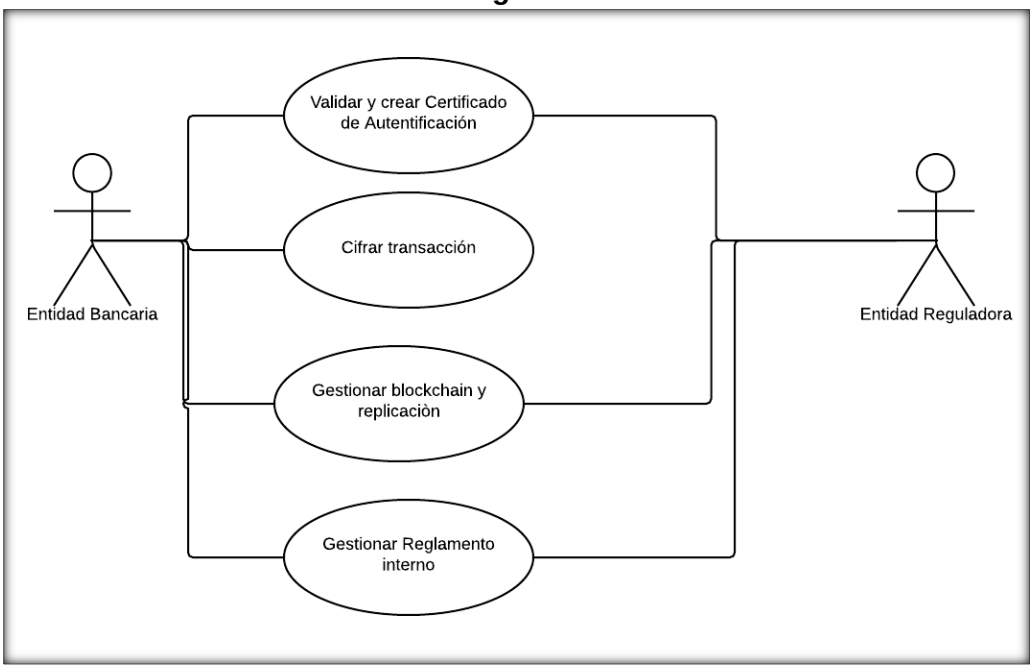
2.1.3. Prototipo del Sistema

2.1.3.1. Diagramas

Casos de Uso

Los cuatro casos que se presentan corresponden a la interacción entre Entidad Bancaria y la Entidad Reguladora que es el Banco Central del Ecuador.

Ilustración 7: diagrama casos de uso

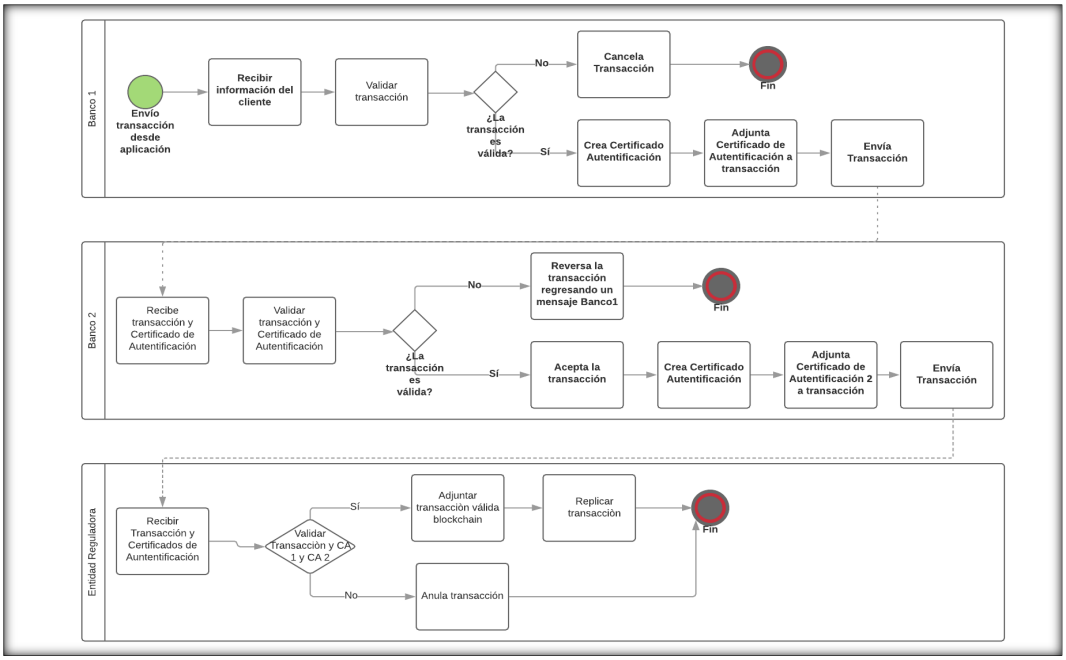


Fuente: Mónica Vargas, 2020.

Diagramas de procesos

El primer paso a la interacción es crear un certificado de autentificación que sea validado por la Entidad reguladora, que permita confirmar la identidad de la Entidad Bancaria que interactúa con el sistema.

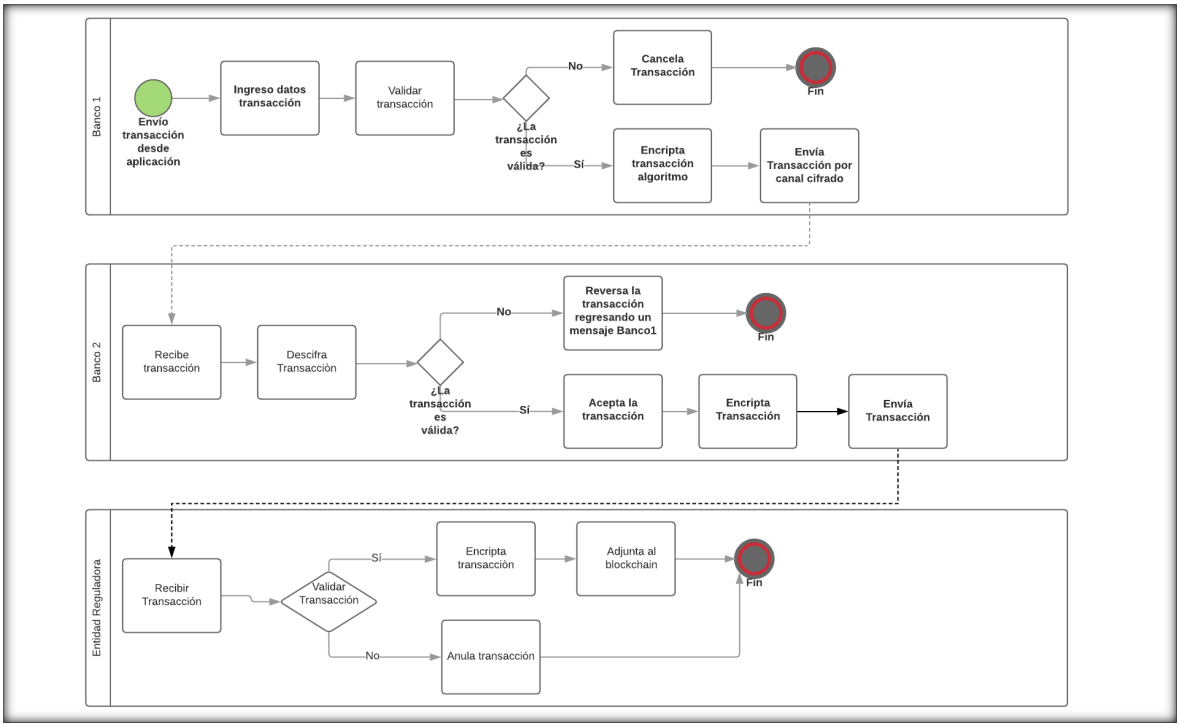
Ilustración 8: validar y crear Certificado de Autentificación



Fuente: Mónica Vargas, 2020.

Una vez valida la transacción por los sistemas internos de cada entidad bancaria, se cifra la transacción para ser trasmitida a la entidad reguladora.

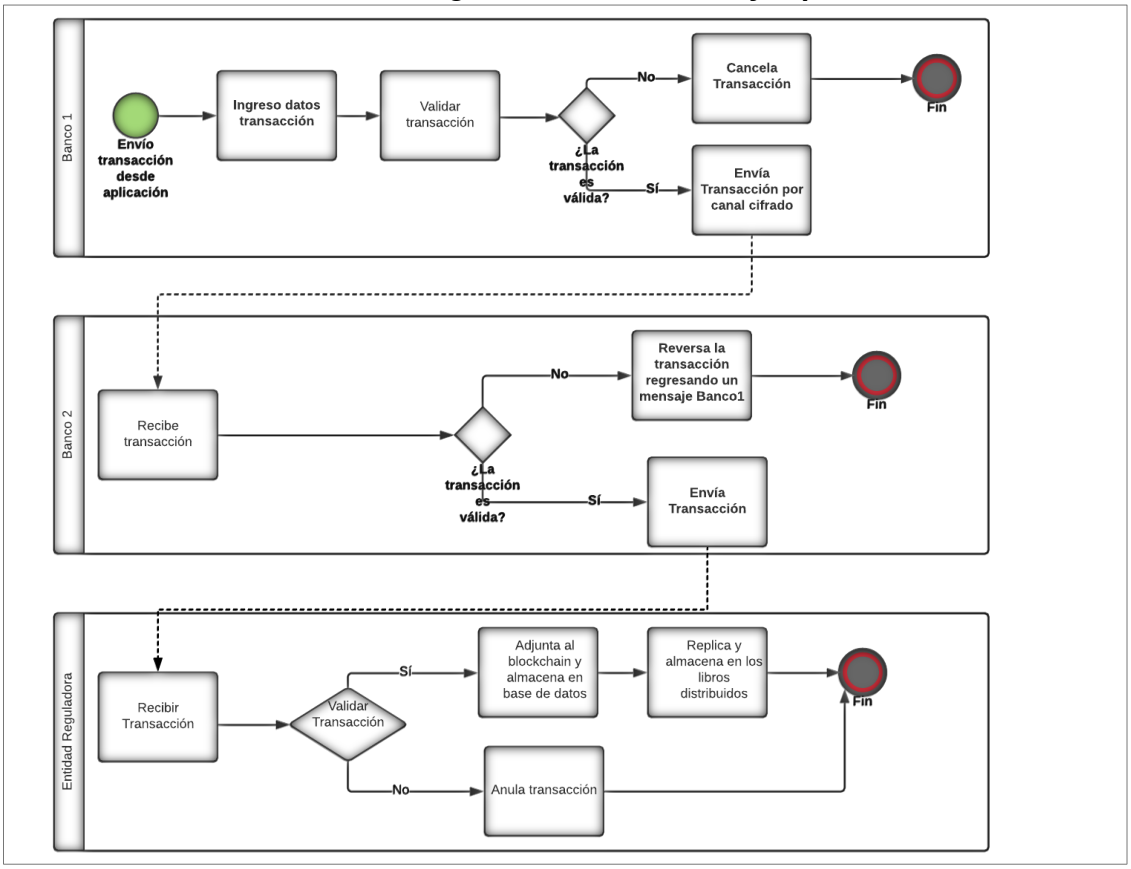
Ilustración 9: cifrar transacción



Fuente: Mónica Vargas, 2020.

La entidad reguladora debe aceptar, de acuerdo a los concesos internos que realiza con cada una de las entidades bancarias, y aceptar la transacción para que se pueda adjuntar al blockchain y posteriormente replicada al sistema distribuido.

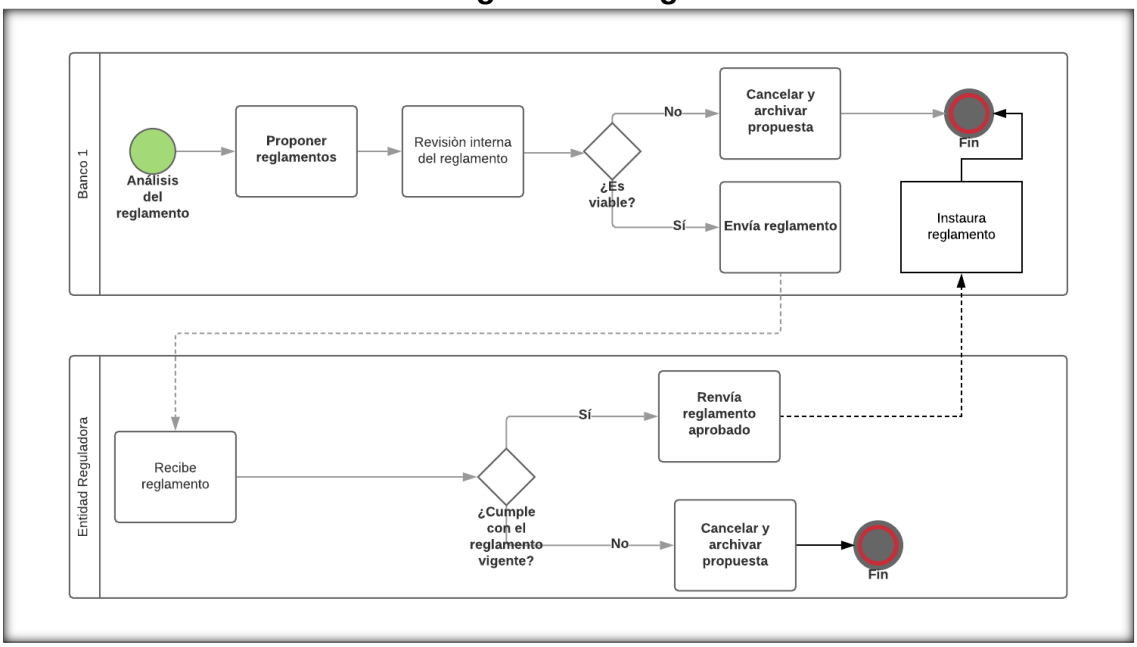
Ilustración 10: gestionar blockchain y replicación



Fuente: Mónica Vargas, 2020.

Cada entidad bancaria puede crear sus propias reglas a ser aprobadas por la entidad reguladora.

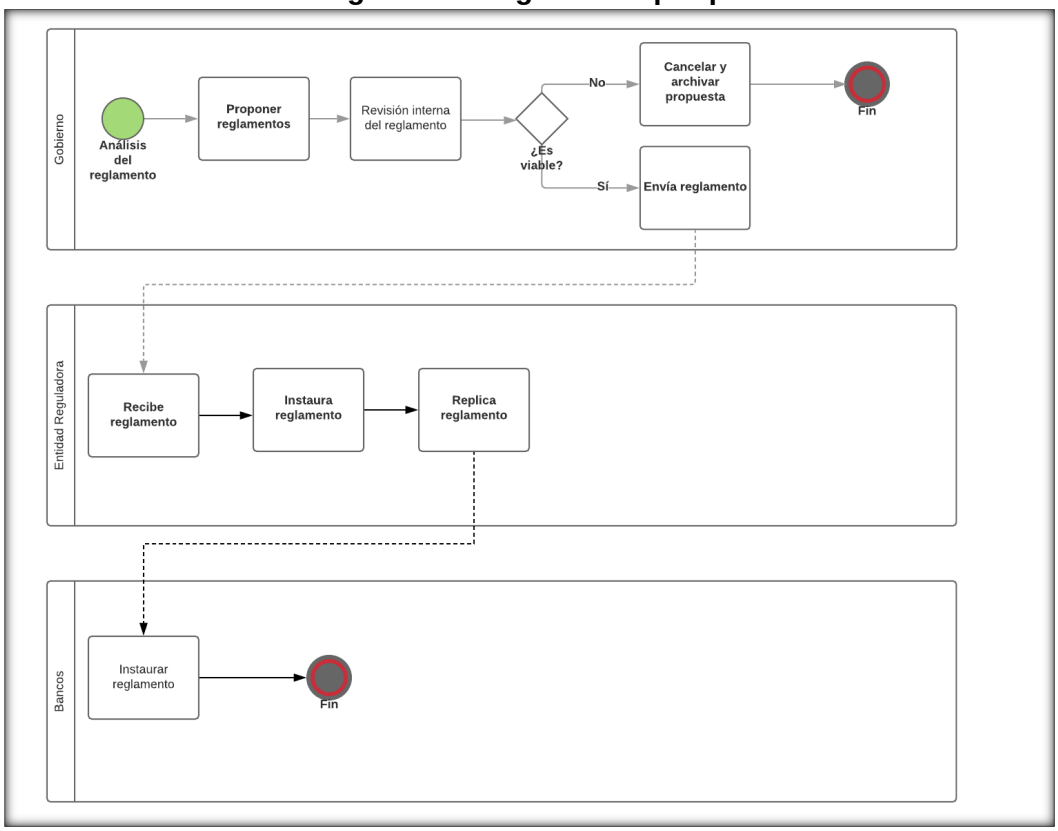
Ilustración 11: gestionar reglamento interno



Fuente: Mónica Vargas, 2020.

En ciertos casos, la entidad reguladora debe colocar reglamentos en forma generalizada para todas las entidades bancarias.

Ilustración 12: gestionar reglamento por pedido externo

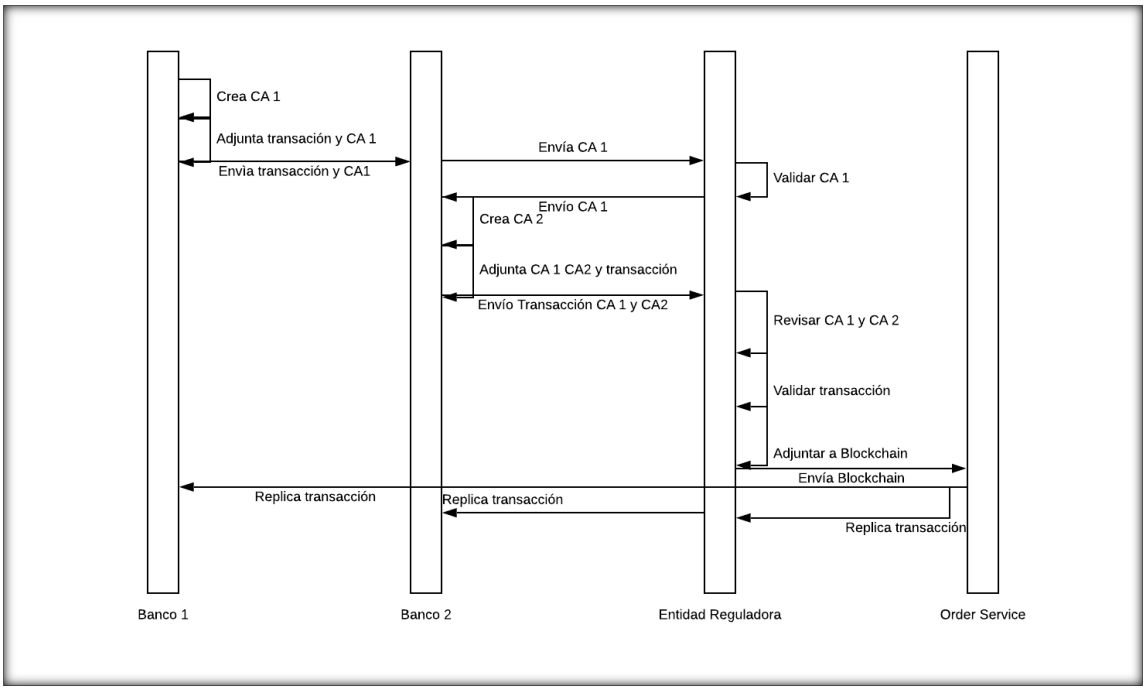


Fuente: Mónica Vargas, 2020.

Diagramas de secuencia

A continuación, se presenta la secuencia que sigue la creación de los certificados de autentificación y su respectiva validación.

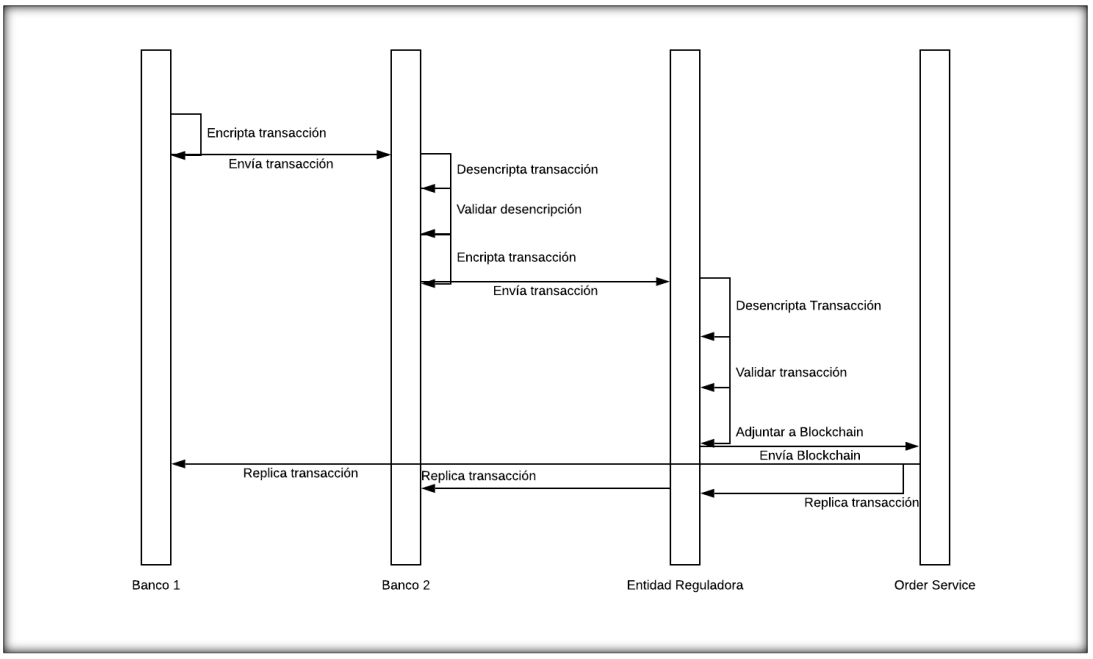
Ilustración 13: secuencia crear Certificado Autentificación



Fuente: Mónica Vargas, 2020.

El diagrama demuestra la transacción siendo encriptada por la entidad bancaria y siendo desencriptada por la entidad reguladora aprobada, adjuntadose al blockchain y siendo replicada.

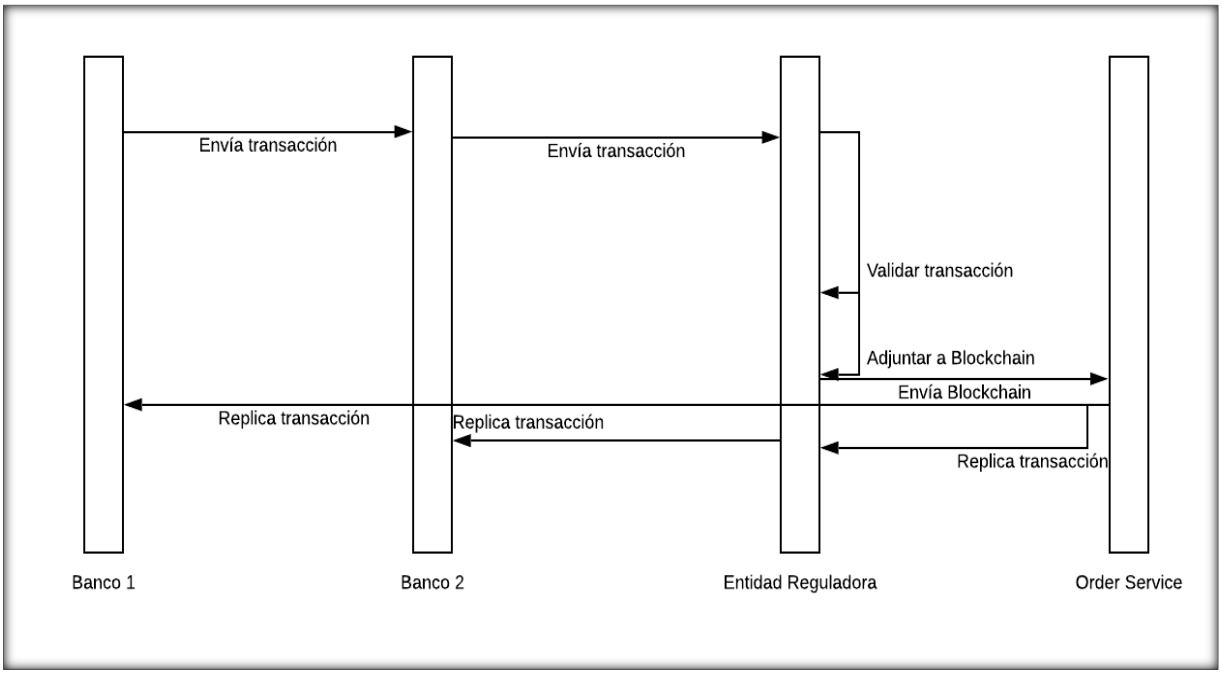
Ilustración 14: secuencia cifrar transacción



Fuente: Mónica Vargas, 2020.

Sólo la entidad bancaria donde se originó el blockchain puede ingresar a la información generada, pese a que ha sido replicada a la base distribuida en varias entidades bancarias.

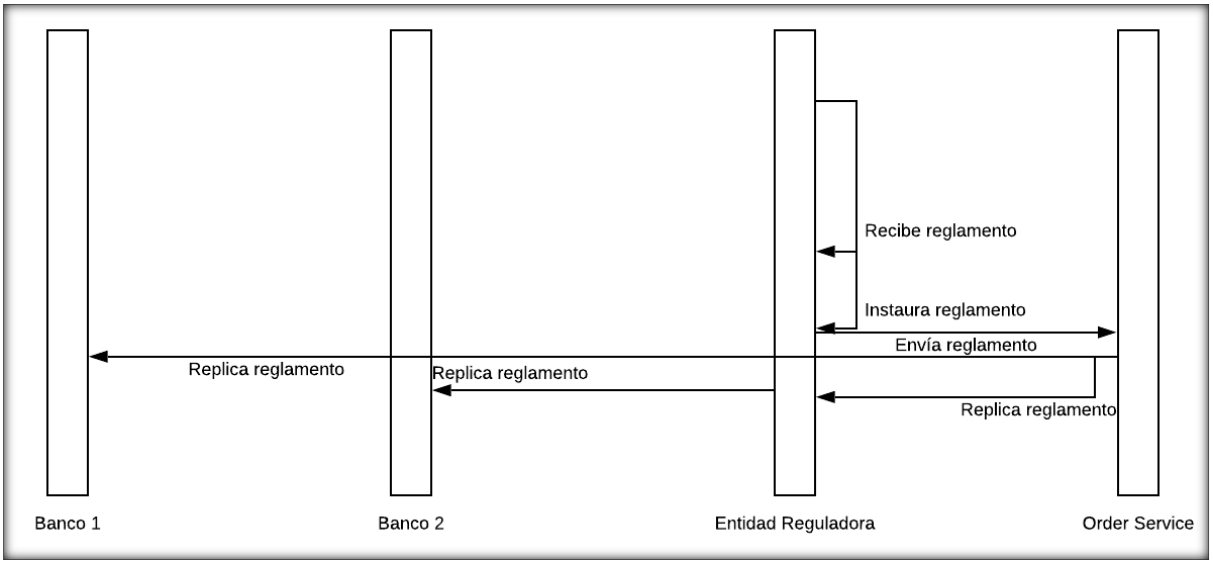
Ilustración 15: secuencia gestionar Blockchain



Fuente: Mónica Vargas, 2020.

El reglamento puede ser realizado por la entidad reguladora y debe ser replicado en todas las entidades bancarias intervinientes, por lo qué la entidad reguladora puede imponer los reglamentos.

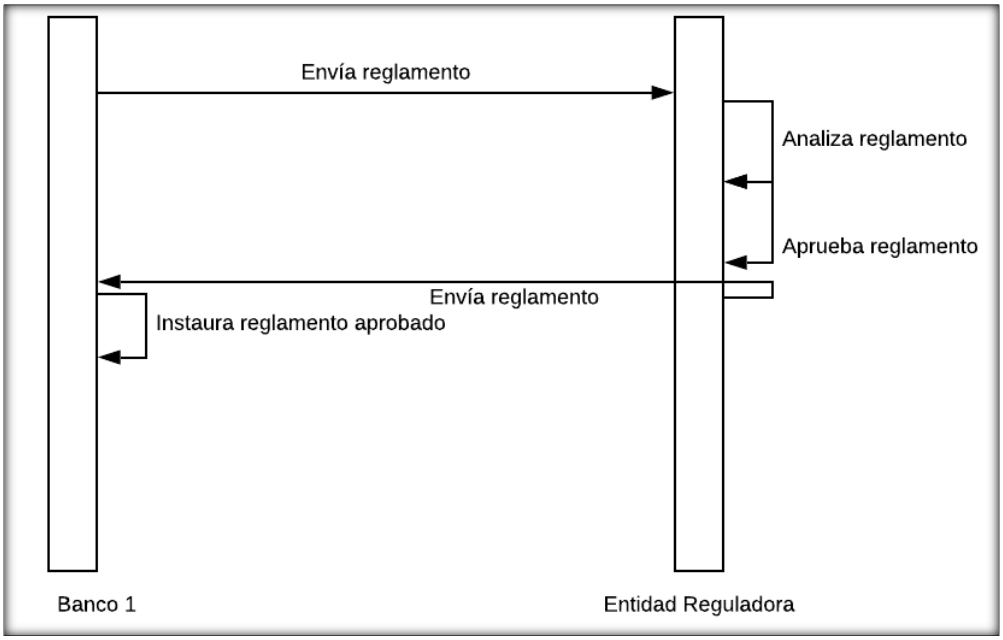
Ilustración 16: secuencia gestión reglamento



Fuente: Mónica Vargas, 2020.

Los reglamentos deben poder incorporarse internamente en las entidades bancarias pero deben ser aprobados previamente por la Entidad reguladora.

Ilustración 17: secuencia gestión reglamento interno



Fuente: Mónica Vargas, 2020.

2.1.3.2. Funcionamiento

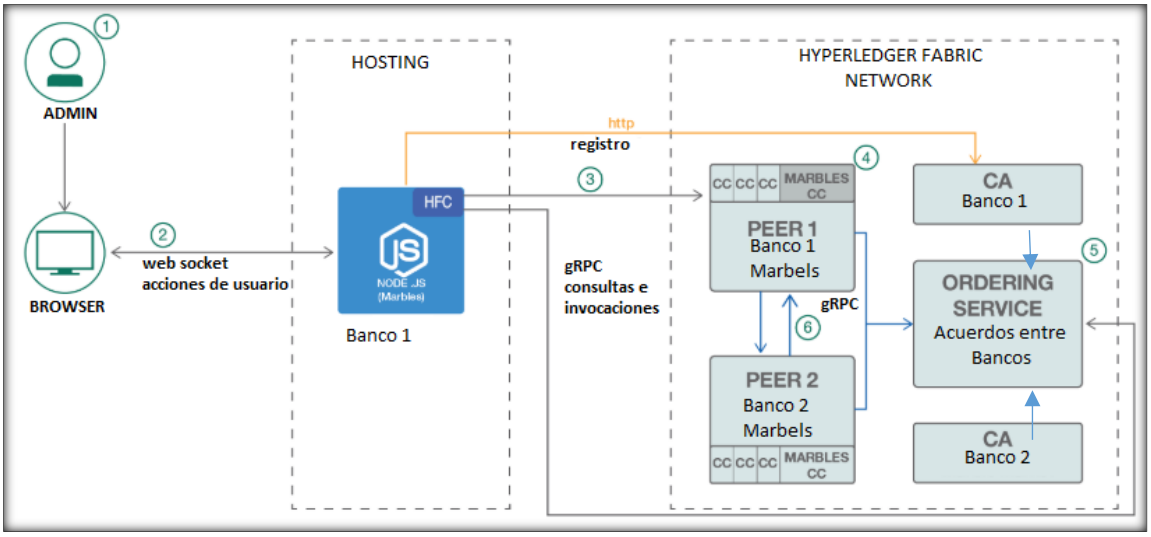
Una aplicación que utilice NodeJs y Go crea un frontend y un backend donde se reflejan las transacciones que se realizan en cada una de las instituciones bancarias, teniendo cómo entidad reguladora al Banco Central del Ecuador en la red blockchain. De esta forma se crean transacciones por medio de marbels, n este caso serían los montos por transferirse de dinero electrónico. Todo queda almacenado en el blockchain, dando seguridad de integridad de datos y no repudio.

Descripción de pasos aplicativos:

1. es el protocolo de criptografía consiste en registrar la identidad del usuario, una identidad peer y la identidad mixta.
2. Solicitud de transacción por medio de un administrador a realizar con Marbels y la aplicación Node JS.
3. Proceso de transacción del cliente en el que se ejecuta de fondo websocket enviando mensajes al backend cuando se interactúa con el sitio.

4. El peer se comunica con el contenedor de Marbels Chaincode y simula la transacción Si no tiene errores y es aprobada, se respalda la transacción y la envía a la aplicación
5. Envía la propuesta respaldada al ordening service que empaqueta las ordenes en bloques y los envía a la red
6. Finalmente, se realiza la actualización de estados en el libro de contabilidad general y sus copias en cada institución bancaria.

Ilustración 18: diagrama de despliegue



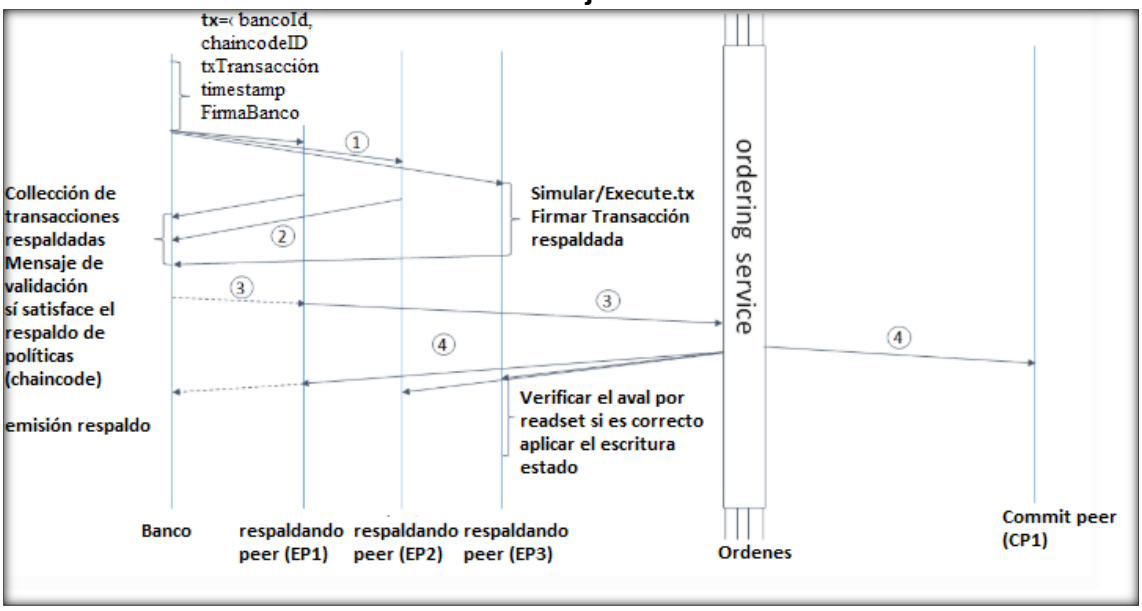
Fuente: (IBM, 2018)

Existen dos tipos de transacciones:

- Despliegue de transacciones en la que se obtiene los datos de parámetros de las aplicativos de los bancos, creando un nuevo chaincode.
- Invocar transacciones que se refiere a invocar la transacción anterior del chaincode y a actualizar el estado en el libro de contabilidad.

El flujo común de cada transacción se realiza por medio de una gráfica que demuestra como al ejecutarse y verificarse, la transacción se respalda en cada peer que participa y en el libro de contabilidad.

Ilustración 19: flujo de transacción

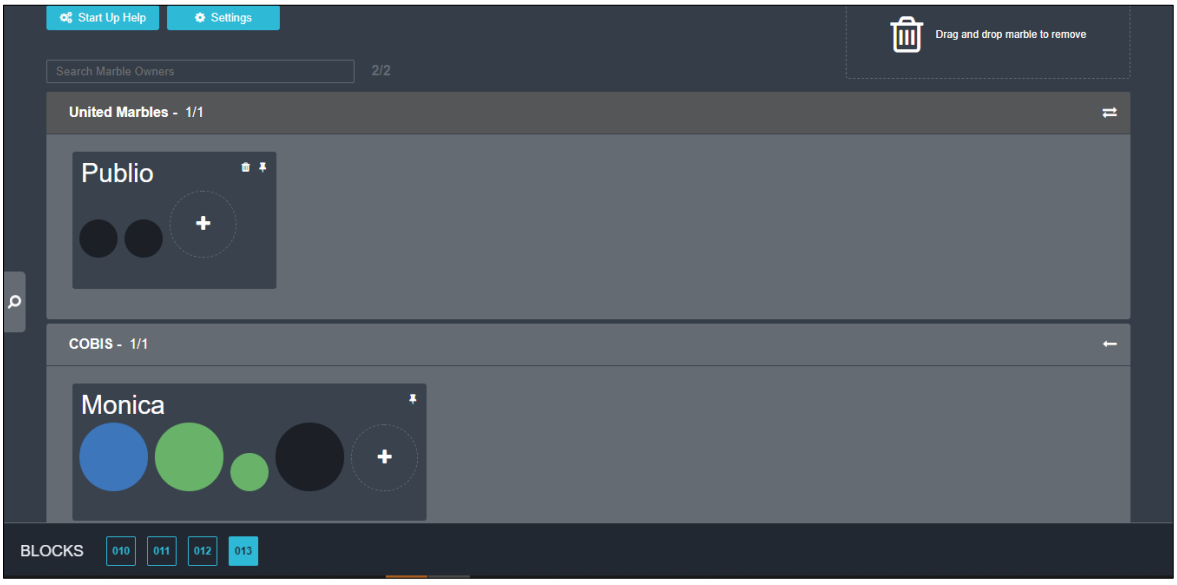


Fuente: (IBM, 2016)

2.1.3.3 Pruebas Prototipo

La creación de entidades bancarias incluyendo clientes ficticios. Y realización de transacciones como se demuestra en las siguientes facturas presentando el bloque de auditoría que demuestra el blockchain.

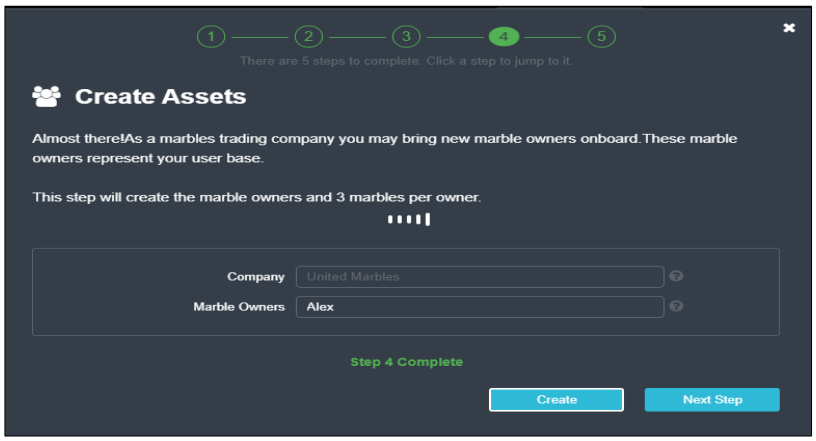
Ilustración 20: Funcionamiento entidades



Fuente: Mónica Vargas, 2020.

Creación de un usuario se puede dar con un identificador o un nombre y eligiendo previamente la entidad bancaria

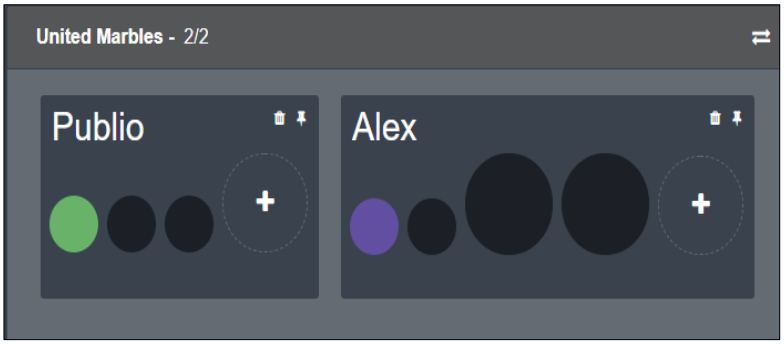
Ilustración 21: Creación usuario



Fuente: Mónica Vargas, 2020.

Una vez que se ha creado se puede agregar o eliminar cualquier transacción que en este caso se representan con círculos

Ilustración 22: Usuario en la entidad



Fuente: Mónica Vargas, 2020.

Puede hacerse una transferencia entre cada uno de los clientes de una misma entidad

Ilustración 23: Ingreso en el usuario

Fuente: Mónica Vargas, 2020.

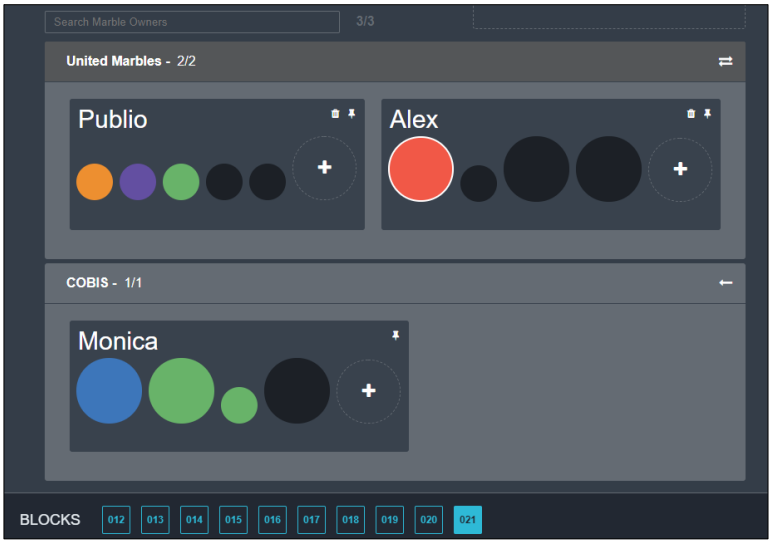
El momento en que se realiza la transacción se emite el código del blockchain como se puede observar en la parte inferior

Ilustración 24: Registro de transacción

Fuente: Mónica Vargas, 2020.

Creación de una transferencia interbancaria

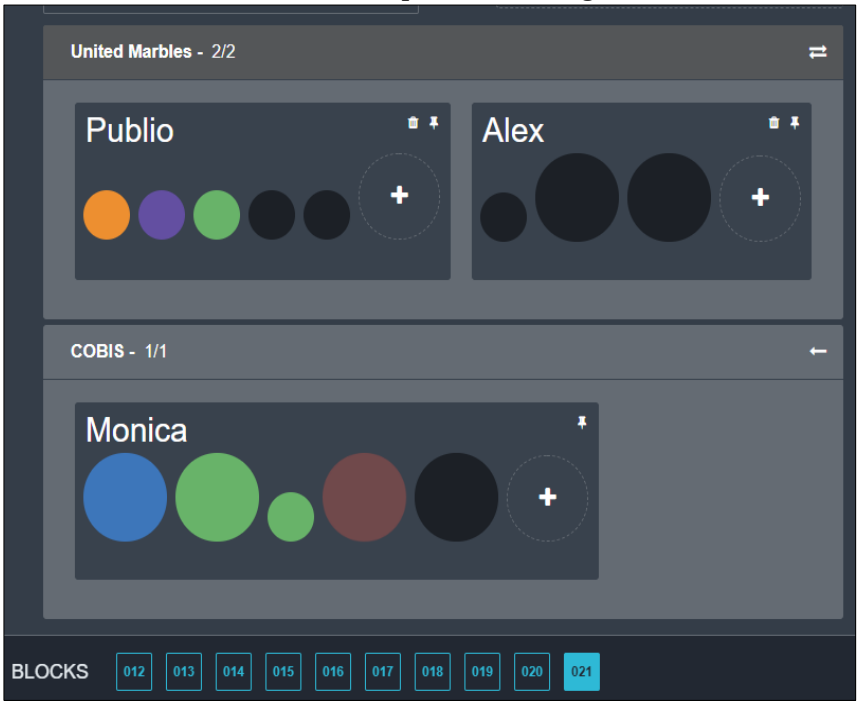
Ilustración 25: Creación nueva transacción



Fuente: Mónica Vargas, 2020.

Mientras la transferencia interbancaria pues realiza las verificaciones pertinentes

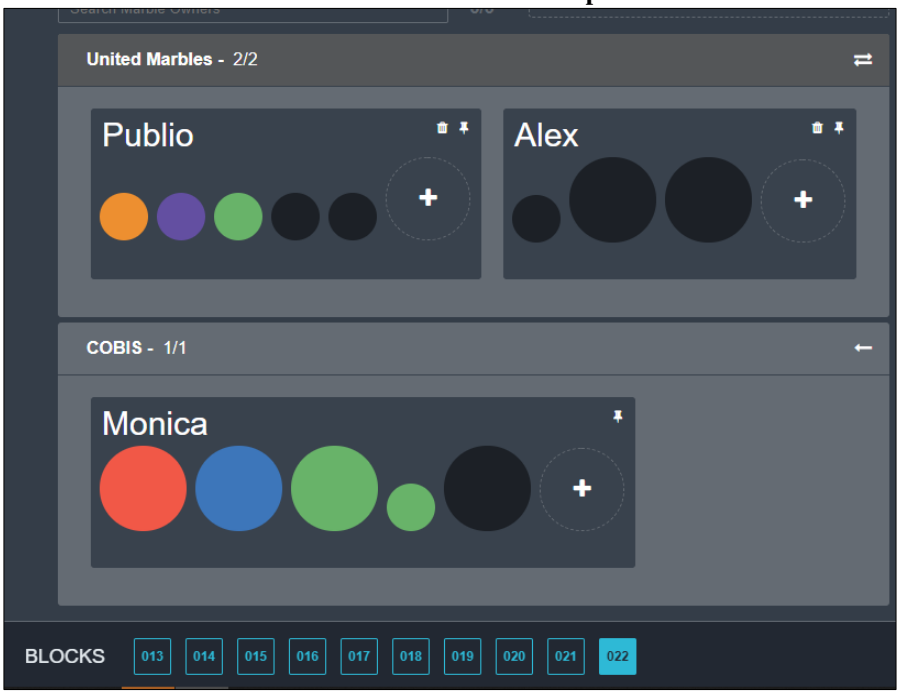
Ilustración 26: Comprobación de reglamento



Fuente: Mónica Vargas, 2020.

Cuando ha pasado las pruebas pertinentes de ambas entidades se tiene las aprobaciones se agrega en el blockchain

Ilustración 27: Transacción comprobada



Fuente: Mónica Vargas, 2020.

El módulo cuenta con auditoría que permite revisar las transacciones realizadas desde cualquiera de las entidades bancarias

Ilustración 28: Auditoría de la transacción

Fuente: Mónica Vargas, 2020.

2.2. Seguridad

Al inicializar el proyecto, se planteó realizar pruebas de etical hacking. Sin embargo, el prototipo contempla varios puntos que mitigan amenazas, cómo por ejemplo: libros de contabilidad distribuidos que impiden su modificación a menos que en la sincronización todos concuerden, canales de intercambio de información encriptada, información encriptada y encadenada por blockchain. La demostración de seguridad del prototipo se realizará comparando las vulnerabilidades que fueron obtenidas de estudios previos realizados por: OWASP, Red Hat y Telefónica. En la tabla 7 se se puede observar las vulnerabilidades que aplican para el proyecto en contraste con las medidas de mitigación realizadas por Hyperledger Fabric.

Tabla 7: vulnerabilidades mitigadas

Vulnerabilidad	Mitigación
Man in the Middle	Los canales conectan con cada peer que se permite teniendo un control de acceso, en caso de lograr interferir el canal cifrado
SQL injection	Este ataque en el aplicativo no se puede realizar ya que para poder realizar una inserción a cualquier tabla del aplicativo se debería realizar por medio de los blockchain anteriores
Robo de Identidad	Cuando se roban credenciales la Autentificación de Certificados puede denegar el acceso y crear una nueva y toda transacción al ser registrada puede rastrearse y eliminarse.

Vulnerabilidad	Mitigación
Fuerza Bruta	El tiempo y costo estimados para este ataque en aumenta con cada bloque que se adhiere a la cadena de blockchain
DoS	Denegación de Servicio al ser un sistema distribuido sí cada institución bancaria posee las transacciones y en espera de la siguiente las transacciones negadas
Robo cibernético y Base de datos	En caso de darse un robo cibernético a un banco específico el Estado Mundial se actualiza en cada peer por lo que deberían atacarse a todos los peers

Fuente: Mónica Vargas, 2020

2 Discusión

Los productos de dinero electrónico tienen el potencial de proporcionar importantes beneficios a los sistemas de pago, si se implementan con la seguridad adecuada. Estos sistemas no pueden ser completamente seguros contra todo tipo de ataque. La determinación del nivel de seguridad apropiado para un sistema en particular, debe incluir la consideración de la magnitud de los riesgos potenciales, el costo de implementar diferentes niveles de seguridad, el impacto en la funcionalidad del producto y las implicaciones para la privacidad.

Además, el uso de dinero electrónico se ha hecho más evidente como lo señala Valdez (2015) en su investigación realizada en la provincia de Manabí, en la que señala *"el dinero electrónico es una ventaja para el desarrollo del comercio ya que aseguran que el país pueda proyectarse a nuevos mercados incursionando en ellos y logrando así beneficios".* Adicionalmente es importante mencionar que los medios electronicos agilizan los procesos y ayudan a la ingración de varios mercados en la economía.

En el sistema criptográficamente seguro de dinero electrónico se encuentran varios puntos que mitigan amenazas, cómo por ejemplo: libros de contabilidad distribuidos que impiden su modificación a menos que en la sincronización todos concuerden, canales de intercambio de información encriptada e información encriptada y encadenada por blockchain. Para esto se considera la investigación realizada por Red Hat (2016) en la cual se menciona que en la intercepción pasiva *"se recolectan los datos que pasan entre dos nodos activos en la red mediante interceptación pasiva en la conexión entre los dos nodos"* (Red Hat, 2016). Al respecto, surge la necesidad de integrar un sistema criptográfico que evite este tipo de vulnerabilidad y así proteger la información.A su vez, se ha observado que el internet es usado cada vez más para el comercio, y con ese uso se evidencian más ataques a la seguridad del sistema para obtener ganancias monetarias. Para Amarasiri &

Dias (2015) *“en comparación con el comercio en el "mundo real", el comercio en red permite un contacto personal reducido, facilidad para escuchar, la capacidad de los atacantes para extraer automáticamente información confidencial de los mensajes y una fácil copia y codificación de datos”*. A medida que estas debilidades se exploten cada vez más, se ve un mayor énfasis en la integración de mecanismos de seguridad con aplicaciones y servicios de red.

Gran parte de la tecnología necesaria para proteger los sistemas de red ya existe. Las técnicas criptográficas se pueden aplicar en apoyo de autenticación, autorización, integridad, confidencialidad, garantía y pago. Sin embargo, para que sea útil, la infraestructura que soporta estas tecnologías debe establecerse, y la tecnología debe integrarse con aplicaciones y protocolos para el comercio electrónico y las estrategias de ataque más exitosas contra ellos; incluyendo transacciones junto con una revisión del estándar dominante, es decir, que incluye varias investigaciones para determinar varios tipos de los ataques que puedan existir.

También se obtuvo que la diferencia del prototipo del sistema presentado es el libro de contabilidad. Los bancos deben cada día realizar cierre de sus operaciones y enviar los reportes hacia el Banco Central del Ecuador. Este prototipo tiene un libro de contabilidad que permite a una entidad reguladora obtener esta información en tiempo real. Inclusive podría permitir una relación con una entidad futura, por ejemplo con el Sistema de Rentas Internas, para evitar la evasión de impuestos al tener una información procesada inmediata de los estados transaccionales.

El software **EFECTIVO** interactuaba sólo con usuarios que contaban con una cuenta en el Banco Central del Ecuador. El prototipo presentado en este documento puede adaptarse a cada uno de los servidores de los bancos o empresas que lo requieran, con la característica de un estado mundial que permite saber sí las transacciones son viables.

Por otro lado, Hyperledger Fabric es una plataforma que permite transacciones de distinta índole. Para el presente prototipo se ha considerado esta plataforma debido a los beneficios que aporta a la implementación reglas, la creación de certificados de autentificación y la transmisión por canales seguros e información encriptada. Por su parte NIST acompaña durante el ciclo de vida del software, como por ejemplo en la creación o mejoramiento de algoritmos de encriptación.

3 Conclusiones

- El dinero electrónico al término de la investigación no se encuentra en funcionamiento en el Ecuador. Sin embargo, el proyecto se puede aplicar a las transacciones realizadas actualmente en transferencias bancarias, tarjetas de crédito o pagos.
- La seguridad informática requiere de avances constantes. La prevención y mitigación deben incluirse en cada paso del ciclo de vida del software por lo que.Al implementar cualquier software se debe proteger las vulnerabilidades con la configuración adecuada de los servidores y redes que se utilicen en cada institución bancaria.
- Este prototipo podría colaborar con un monitoreo que permita evitar los delitos de transferencias ilícitas en los bancos, ya que la información está disponible para consultar en tiempo real en cada una de las instituciones.
- Un sistema distribuido del prototipo presenta la ventaja de que al ser atacado uno sólo de los libros, puede recuperarse el mismo al tener un estado global en cada una de las instituciones qué contarían con el servicio.

Bibliografía

- Acosta-Veliz, M., Guerra-Tejada, A., & Viteri-Luque, F. (2018). Evolución y perspectivas del dinero electrónico en el Ecuador. *Dominio de las Ciencias*, 569-584.

- Adams, K. (2015). *Non-functional Requirements in Systems Analysis and Design.* Switzerland: Springer International Publishing.

- Amarasiri, R., & Dias, G. (2015). Thechniques for secure electronic transaction. *Department of Computer Science & Engineering, University of Moratuwa* .

- Asimov, M. (1962). *Introduction to design.* Englewood: Prentice-Hall.

- Atwood, M. E., Ramsey, H. R., & Campbell, G. D. (2015). Modern software development methodologies and their environments. *Computer Physics Communications*, 119-134.

- Banco Central del Ecuador. (2011). *INSTRUCTIVO DEL USUARIO DEL GENERADOR DE PAGOS DEL SPI-SP.* Quito.

- Banco Central del Ecuador. (31 de marzo de 2016). *BCE EXPLICÓ INCENTIVOS AL USO DEL DINERO ELECTRÓNICO PROPUESTOS EN NUEVA LEY*. Obtenido de https://www.bce.fin.ec/index.php/boletines-de-prensa-archivo/item/870-bce-explic%C3%B3-incentivos-al-uso-del-dinero-electr%C3%B3nico-propuestos-en-nueva-ley

- Banco Central del Ecuador. (2016). *Inclusión financiera en el Ecuador y las oportunidades de dinero electrónico.* Obtenido de https://www.cepal.org/sites/default/files/events/files/09_jorge_moncayo_-_inclusion_financiera_-_innovacion_de_instrumentos_-_dinero_electronico.pdf

- Banco Central del Ecuador. (30 de agosto de 2017). *Dinero electrónico será manejado por la banca pública, privada y el sistema financiero popular y solidario*. Obtenido de https://www.bce.fin.ec/index.php/boletines-de-prensa-archivo/item/991-dinero-electrónico-será-manejado-por-la-banca-públic

- Barakat, M., Eder, C., & Hanke, T. (2018). *An Introduction to Cryptography.* Kaiserslautern-Alemania: University of Kaiserslautern.

- Bissessar, S. (2016). *Opportunities and risks associated with the advent of digital currency in the Caribbean.* Santiago, Chile: The Economic Commission for Latin America and the Caribbean.

- Cassoni, A. (2013). Digital money and its impact on local economic variables: the case of Uruguay . *Universidad ORT Uruguay*, 1-37.

- COBIS Financial Agility Partners. (01 de enero de 2015). *COBIS.* Obtenido de http://conoce.cobiscorp.com/software-financiero?utm_campaign=MARCA+-+TODOS&utm_source=adwords&utm_medium=ppc&utm_term=cobiscorp&hsa_ad=118136650025&hsa_kw=cobiscorp&hsa_grp=20113307105&hsa_ver=3&hsa_src=g&hsa_mt=p&hsa_acc=2874787589&hsa_net=adwords&hsa_ca

- Código Orgánico Monetario y Financiero. (2014). *Registro Oficial N° 332, 12 de septiembre.* Quito: Asamblea Nacional. Obtenido de http://www.ecuadorlegalonline.com/biblioteca/codigo-tributario/

- Constitución de la República del Ecuador. (2008). *Registro Oficial 449 de 20-octubre.* Quito: Asamblea Nacional.

- Cross, N. (2002). *Métodos de diseño. Estrategias para el diseño de productos.* México DF: Editorial Limusa.
- Cross, N. (2008). *Engineering design methods.* Hoboken : NJ: Wiley.
- Dirección de Auditoría de Tecnología de la Información. (2015). *Informe General al componente de Seguridad del Sistema de Pagos Interbancarios.* Quito: Contraloría General Estado.
- Dixit, U. (2017). Cryptography – Security in E-Banking. *IOSR Journal of Business and Management (IOSR-JBM)* , 33-37.
- El Telégrafo. (01 de enero de 2017). *El dinero electrónico generó más de $ 15 millones en transacciones*. Obtenido de http://tinyurl.com/y9n2wcjm
- Freeman, P. (1980). The nature of design. *Tutorial on Software Design Techniques, Freeman, P. and Wasserman, A. I. Eds, IEEE*, 46-53.
- Freeman, P., & Wasserman, A. I. (1980). *Tutorial on Software Design Techniques.* IEEE.
- Gonzalez-Longatt, F. (01 de agosto de 2012). *uv.mx.* Obtenido de Introducción a los Sistemas de Información : https://www.uv.mx/personal/artulopez/files/2012/08/FundamentosSistemasInformacion.pdf
- Hanácek, P. (2015). Security of Electronic Money. Bozetechova, República Checa: Technical University of Brno.
- Haviluddin, H., & Anthony, P. (2012). *COBIT Framework for Information Technology Governance (ITG) at Mulawarman University, Samarinda, East Kalimantan, Indonesia: A Descriptive Study.*
- IBM. (01 de marzo de 2016). *Hyperledger Fabric.* Obtenido de Hyperledger Fabric: https://hyperledger-fabric.readthedocs.io/en/release-1.4/blockchain.html
- IBM. (27 de junio de 2018). *IBM Developer.* Obtenido de Blockchain: https://developer.ibm.com/patterns/deploy-an-asset-transfer-app-using-blockchain/
- Law, L., Sabett, S., & Solinas, J. (2016). *La criptografía del efectivo electrónico.* Obtenido de

https://groups.csail.mit.edu/mac/classes/6.805/articles/money/nsamint/nsamint.htm#2

- Machado, G. A. (2010). *Implementación de un sistema de billetera electrónica en el Transporte Colectivo de la ciudad de Porto Alegre.* Porto Alegre - Brasil: Universidad de Porto Alegre.

- Ministerio de Telecomunicaciones y de la Sociedad de la Información . (25 de 11 de 2019). *Libro Blanco de Territorios Digitales en Ecuador .* Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2019/11/LBTD_actualizado_25-11-2019_a.pdf

- NIST. (marzo de 2016). *Cryptographic Technology Group.* Obtenido de NIST Cryptographic Standards and: http://dx.doi.org/10.6028/NIST.IR.7977

- Organización de los Estados Americanos. (2018). *Estado de la Ciberseguridad en el Sector Bancario en America Latina y el Caribe.* Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo.

- Peñaherrera Diego, H. C. (2013). *La aceptación de la billetera móvil en empresas influyentes del Ecuador.* Quito: Universidad San Francisco de Quito.

- Real Academia Española. (24 de marzo de 2020). *Diccionario de la lengua española*. Obtenido de https://dle.rae.es/sistema?m=form

- Red Hat. (05 de abril de 2016). *Vulnerabilidades y ataques comunes*. Obtenido de https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-common_exploits_and_attacks

- Sgarro, A. (1990). *Códigos Secretos.* Madrid: Ediciones Pirámide.

- Syeful, I. (2015). An Algorithm for Electronic Money Transaction Security (Three Layer Security): A New Approach. *International Journal of Security and Its Applications*, 203-214.

- Tata Consultancy Services. (01 de junio de 2019). *TCS BANCS.* Obtenido de https://www.tcs.com/bancs/quartz-blockchain-solutions

- Telefónica Company . (02 de marzo de 2017). *Bases de datos y sus vulnerabilidades*. Obtenido de https://www.acens.com/wp-content/images/2015/03/vulnerabilidades-bbdd-wp-acens.pdf

- Valdez Álvarez, J. V. (2015). *Análisis del impacto financiero del uso de dinero electrónico en el sector de economía popular y solidaria de MAnabí.* Manabí: Universidad Tecnológica Equinoccial (UTE).

- Wasim Munir, M. (2015). *Cripthografía.* Informática. Karachi - Pakistan: Barrett Hodgson University.