Universidad Autónoma de Baja California

Maestría y Doctorado en Ciencias e Ingeniería

Diseño e implementación de un prototipo de sistema en punto de venta (PoS) basado en Blockchain

Tesis

que para cubrir parcialmente los requisitos necesarios
para obtener el grado de

Maestro en Ingeniería

Presenta

José Ramón López Madueño

29 de enero de 2021

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE INGENIERÍA, ARQUITECTURA Y DISEÑO

MAESTRÍA Y DOCTORADO EN CIENCIAS E INGENIERÍA

Diseño e implementación de un prototipo de sistema en punto de venta (PoS) basado en Blockchain

TESIS

Que para obtener el grado de maestría en ingeniería / Doctorado en Ciencias presenta:

José Ramón López Madueño

Aprobada por:

Dr. Christian Xavier Navarro Cota
Director de tesis

Dr. J. Reyes Juárez Ramírez
Co-director de tesis

Dr. Juan Iván Nieto Hipólito
Miembro del comité

Ensenada Baja California, México.
Enero de 2021.

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

Abstracto

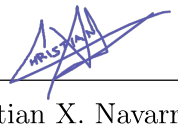
Ingeniería en Computación

Maestría en Ingeniería

Diseño e implementación de un prototipo de sistema en punto de venta (PoS) basado en Blockchain

por José Ramón López Madueño

Aprobado por



Dr. Christian X. Navarro Cota
Director de Tesis

Dr. J. Reyes Juárez Ramírez
Co-director de Tesis

Abstracto

Actualmente, existen aplicaciones de pago basados en Blockchain, y que podrían adaptarse para obtener un sistema de Punto de Ventas (PoS, por sus siglas en inglés). Sin embargo, estas aplicaciones son pruebas de concepto o prototipos que son propuestos por la comunidad en esta área, por ejemplo, el comercio electrónico. Otro problema detectado es que estas aplicaciones no consideran otros tipos de pago, es decir, solo permiten pagos con dinero digital y no con dinero tradicional (fíat). Asimismo, no contemplan el proceso de intercambio entre estos dos tipos de dinero. Finalmente, no se encontró literatura científica relacionada a este tema de interés. Esta tesis propone desarrollar un marco conceptual y proporcionar una API que detalle el diseño de un sistema de pagos en un PoS utilizando una instancia de Blockchain, considerando diferentes tipos de pagos e intercambios de dinero, así como la evaluación de su viabilidad. El resultado de esta investigación proveerá a pequeñas y medianas empresas de una forma rápida y sencilla de implementar un sistema de esta índole en sus distintos establecimientos, junto con todos los beneficios que ofrece esta tecnología, como lo es el costo de transacción y operación, la confirmación instantánea y la seguridad de las transacciones, así como su alta liquidez.

"The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts."

Satoshi Nakamoto

Índice general

Índice de figuras

Índice de cuadros

1 Introducción

1.1. Introducción

Las monedas digitales proponen un cambio fuera de los diseños de infraestructura establecidos en el sistema financiero. Los sistemas de información y las soluciones tecnológicas, como la conectividad entre pares (P2P) y los algoritmos criptográficos, permiten la organización descentralizada, la seguridad operacional y la transparencia, oponiéndose a las estructuras tradicionales de los sistemas monetarios centralizados y poco transparentes [38]. En el contexto de la reciente crisis económica, esta nueva casta de monedas está ganando la atención del público. A medida que se disminuye la confianza del público en la actual estructura del sistema financiero, los conceptos alternativos se vuelven más y más relevantes e introducen conceptos innovadores para los sistemas monetarios futuros.

La moneda digital que atrae la mayor atención en este contexto es Bitcoin, propuesta por un usuario bajo el seudónimo de Satoshi Nakamoto [32]. Bitcoin es un mecanismo financiero electrónico que proporciona características que se asemejan a un sistema monetario establecido con su propio régimen de creación y transacción de dinero, pero que se basa en una estructura organizacional descentralizada. En contraste con la toma de decisiones en un banco central, la creación de dinero en el sistema Bitcoin se realiza de manera transparente mediante un algoritmo abierto y distribuido. Asimismo, la infraestructura permite el monitoreo de transacciones casi en tiempo real a través de una red pública y distribuida. Todo el historial de transacciones se almacena en una 'cadena' [32] de transacciones, denominado Blockchain.

1.2. Problemática

Blockchain ha alcanzado un nivel de adopción nunca visto. Sin embargo, la comunidad académica no ha prestado atención a aplicaciones de sistemas de pagos en el mundo real —más específicamente, terminales de punto de venta basadas en Blockchain— y a sus requisitos únicos en términos de seguridad, usabilidad e implementabilidad.

Dentro de la literatura se hace referencia a pagos escalables en Blockchain utilizando entornos de ejecución de confianza [26] o a protocolos de consenso que optimizan las transacciones [24], sin embargo, no se hace mención de sistemas de pagos en punto de venta, es decir, no existe alguna metodología o modelo que permita implementar o desarrollar un sistema de este tipo. Aunque existen pruebas de concepto en el mundo real, existe una falta y una necesidad de un marco teórico que describa el diseño y evaluación de dichos sistemas. Asimismo, al observar las propuestas e implementaciones de los sistemas de pago actuales, se detecta que no cubren la parte de intercambio entre la moneda digital que se esté utilizando y el dinero fiduciario[1], y funcionan más como una prueba de concepto.

[1] Dinero emitido por el gobierno.

1.3. Justificación

Actualmente, existen aplicaciones de pago en blockchain que podrían adaptarse a un sistema PoS, y varios prototipos y pruebas de concepto propuestas por la comunidad en esta área, sin embargo, no se cuentan con fundamentos teóricos que justifiquen tales sistemas. Asimismo, en la literatura no se hace referencia al proceso de intercambio entre el dinero digital al tradicional, y viceversa.

Esta tesis propone diseñar e implementar un sistema de pagos en puntos de venta utilizando una instancia de Blockchain, y realizar una evaluación de su viabilidad.

El resultado de esta investigación proveerá a pequeñas y medianas empresas de una forma rápida y sencilla de implementar un sistema de esta índole en sus distintos establecimientos junto con todos los beneficios que ofrece esta tecnología, como lo es el costo de transacción y operación, la confirmación instantánea y la seguridad de las transacciones, así como su alta liquidez.

1.4. Antecedentes

Para los propósitos de este trabajo, se realizó una investigación del panorama literario actual en el campo de las tecnologías de la información con relación a Blockchain, más específicamente, al sector financiero tomando como contexto un sistema de pagos en punto de venta basado en una implementación de Blockchain. Dentro de estas investigaciones, Blockchain aún se considera una innovación y no se ha establecido como una investigación dentro del área. Además, motivados por la naturaleza técnica y matemática de Blockchain, la mayor parte de la investigación previa se ha centrado exclusivamente en aspectos de infraestructura tecnológica, como la seguridad, el anonimato, la escalabilidad o la flexibilidad de los protocolos de consenso[2].

Monedas digitales

Antes del surgimiento de Bitcoin, ha habido varios ejemplos de monedas digitales que han atraído mucha atención. Estas monedas tienen un diseño en un entorno cerrado, por ejemplo, los juegos en línea, y están diseñadas para ser una oportunidad de pago dentro de estos entornos específicos. Kaplanov [20] llega a la conclusión de que Bitcoin se parece más a una moneda de la comunidad. La investigación realizada en esta área, sin embargo, proporciona resultados alejados relacionados con la utilización y el comportamiento.

Autoridades como el Servicio de Impuestos Internos (IRS, por sus siglas en inglés) y el FinCEN (Financial Crimes Enforcement Network) reconocen a Bitcoin como una moneda vitual (convertible) con respecto a su funcionalidad, pero lo distinguen de una moneda "real" debido a que no se define como moneda de curso legal en cualquier país [33].

Por ejemplo, la moneda digital Linden Dollar que tiene sus raíces en el mundo virtual de *Second Life*[3] experimentó una popularidad y atención por los medios similar a Bitcoin. Ernstberger [13] analiza las políticas del dinero virtual basadas en el dólar Linden. Encuentra que los dólares Linden se utilizan como un equivalente al dinero y, por lo tanto, extienden el gasto de dinero hacia un entorno virtual. Dicho de otra manera, descubre que los usuarios de la comunidad de Second Life gastan dinero de una manera similar a la forma en que la gente gasta dinero en el mundo real. Como la economía de Second Life está vinculada a la plataforma, las investigaciones anteriores ignoran los aspectos técnicos-económicos de Linden Dollar, pero se centran en su potencial como entorno virtual para la educación y el aprendizaje [54]. Las investigaciones anteriores no abordaron los efectos económicos del dólar Linden, ya que Second Life se considera principalmente

[2] Los algoritmos de consenso permiten a una red descentralizada llegar a un consenso acerca del estado y orden de llegada de las transacciones.

[3] https://secondlife.com/

como un paradigma de aprendizaje respaldado por una moneda de la comunidad virtual [31]

Otro ejemplo de una moneda digital más exitosa es el oro virtual utilizado en el ecosistema virtual del juego multijugador masivo *World of Warcraft*[4].

Si bien estas monedas tuvieron bastante éxito dentro de su propio entorno, nunca lograron una extensión hacia el mundo real, debido al diseño cerrado de estos sistemas. Bitcoin permite analizar el surgimiento de una moneda digital en un entorno abierto y descentralizado, y permite análisis analíticos y empíricos más amplios.

[4] https://worldofwarcraft.com/es-mx/

1.5. Objetivos

Objetivos generales

Diseñar e implementar un sistema de punto de venta basado en Blockchain, que cubra el flujo desde la recepción de una criptomoneda en un establecimiento hasta el intercambio por dinero tradicional.

Objetivos específicos

1. Analizar y clasificar las propuestas y aplicaciones provistas por la comunidad para obtener un panorama sobre las condiciones del mercado.
2. Definir los requerimientos necesarios para el diseño de un sistema PoS y los criterios que mejor se adapten a un sistema basado en Blockchain.
3. Definir los requerimientos para lograr el intercambio criptomoneda-fiat en el entorno de un sistema PoS.
4. Diseñar el sistema considerando todos los requerimientos definidos anteriormente.
5. Implementación del sistema PoS en Blockchain.
6. Realizar pruebas al prototipo del sistema.

1.6. Preguntas de investigación

Esta investigación pretende resolver las siguientes interrogantes:

- ¿Es posible establecer una guía o metodología que permita la implementación de un punto de venta basado en Blockchain?
- ¿Cuáles son los requisitos necesarios para permitir el intercambio del dinero digital al dinero tradicional, y viceversa?
- ¿Cuáles requisitos deben tomarse en cuenta para el diseño de un sistema de punto de venta en Blockchain?

2 Estado del arte

2.1. Blockchain

Blockchain es el registro público de todas las transacciones de Bitcoin que se hayan ejecutado. Crece constantemente a medida que los mineros agregan nuevos bloques a la cadena (cada 10 minutos aproximadamente) registrando las transacciones más recientes. Los bloques se agregan a la cadena de bloques en un orden lineal y cronológico. Cada nodo completo (es decir, cada computadora conectada a la red utilizando un cliente que realiza la validación y transmisión transacciones) tiene una copia de la cadena de bloques, que se descarga automáticamente cuando un minero se une a la red Bitcoin. Blockchain tiene la información completa de direcciones y balances desde el bloque génesis (el primer bloque de la cadena) hasta el bloque más reciente. La cadena de bloques como un libro contable significa que es fácil consultar cualquier explorador de bloques (como https://www.blockchain.com/explorer) para observar el historial completo de transacciones asociadas con una dirección de Bitcoin en particular.

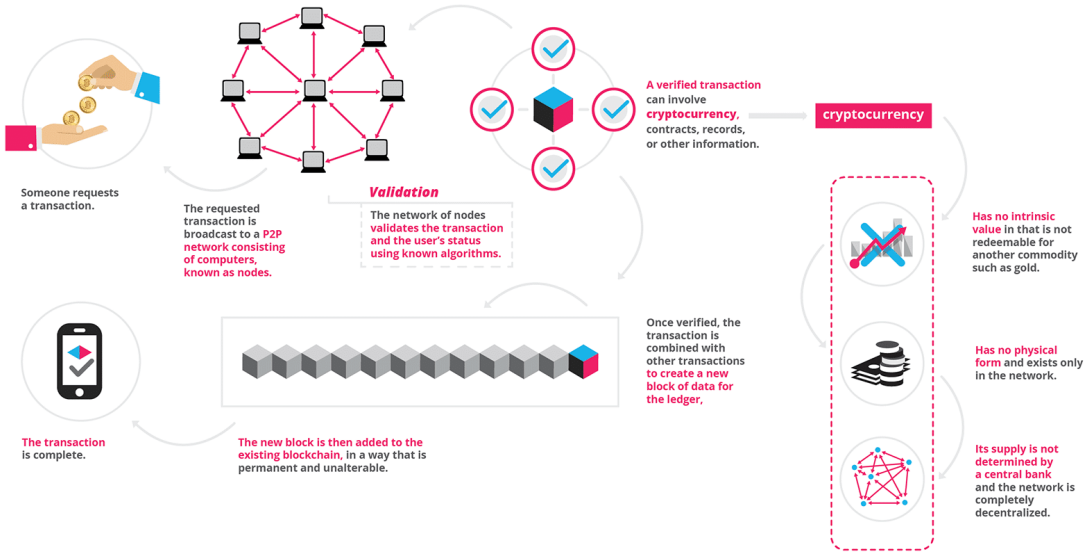


FIGURA 2.1: Flujo de una transacción por medio de Blockchain

Blockchain se considera la principal innovación principal de Bitcoin porque se presenta como un mecanismo de prueba "sin confianza" de todas las transacciones en la red. Los usuarios pueden confiar en el sistema de libro contable distribuido y mantenido a través de muchos nodos conectados entre sí, en lugar de tener que establecer y mantener la confianza con alguna contraparte (otra persona) o un intermediario (como un banco). La cadena de bloques, como la arquitectura para un nuevo sistema de transacciones descentralizadas y sin confianza, es la innovación clave. Blockchain permite la desintermediación y la descentralización de todas las transacciones de cualquier tipo entre todas sus partes a nivel global.

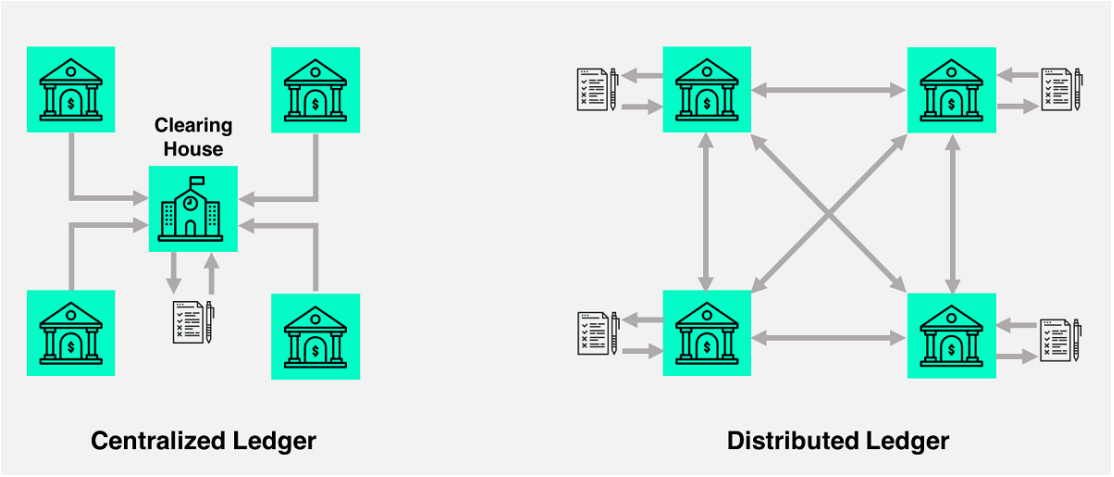


FIGURA 2.2: Comparación de Blockchain con un sistema centralizado

La tecnología Blockchain es como otra capa de aplicación que se puede ejecutar en la pila existente de protocolos de Internet, agregando una capa completa a Internet que permite transacciones económicas, tanto para pagos inmediatos (en un criptomoneda universal) como para contratos financieros más complicados, y a largo plazo. Cualquier moneda, contrato financiero o activo se puede negociar con un sistema como Blockchain. La cadena de bloques se puede utilizar para cualquier forma de registro de activos, inventario e intercambio, incluyendo todas las áreas de finanzas, economía y dinero; activos duros (propiedad física); y activos intangibles (votos, ideas, reputación, datos de salud, etc.).

Características

A la vista de lo anteriormente expuesto, existen tres características de la tecnología blockchain que son especialmente relevantes en el planteamiento de las cuestiones jurídicas que suscitan las aplicaciones de esta tecnología. Estas características son las siguientes:

- **Transparencia**

  Partiendo de la base de que todos los usuarios de las redes blockchain tienen acceso al libro registro, ello implica que todos tienen la información sobre las transacciones que se efectúan por el grupo. Es más, en determinadas redes —no en todas—, los usuarios que no forman parte de la red también pueden consultar el contenido de la cadena de bloques. Así ocurre, por ejemplo, en las redes Bitcoin o Ethereum. A esto se añade, además, que se trata de protocolos informáticos de código abierto, por lo que el acceso al diseño de la programación es también libre. Esta transparencia, sin embargo, no significa que podamos conocer al autor de las transacciones en todo caso. En algunos tipos de redes los usuarios no necesitan identificarse de forma personal para acceder y operar en la correspondiente red blockchain. Las transacciones son visibles, pero vinculadas a un código. Esta característica ha ocasionado que se hayan vinculado algunas de estas redes a actividades ilícitas por el carácter anónimo en la actuación que permiten en ciertos casos.

- **Irrevocabilidad**

  Una vez que la información se incorpora a una red blockchain, en general (salvo ciertas excepciones), no es posible eliminarla de allí. En otras palabras, no hay marcha atrás. La información es poseída por todos los usuarios, por lo que es imposible eliminarla de la red. Los datos incorporados a la cadena de bloques se distribuyen a todos y cada uno de los nodos que intervienen en ella.

- **Inmutabilidad**

  Como consecuencia del encadenamiento sucesivo de los bloques basado en la criptografía (los hash), el contenido de la cadena de bloques es inmutable. Si un nodo decide cambiar el contenido de la cadena de bloques alterando una transacción ya realiza-da e incluida en un bloque, provocará que el con-tenido de su versión del libro registro varíe, un cambio que será fácilmente identificable por el resto de los nodos. Por lo tanto, a la hora de someter a aprobación una nueva transacción, estos no aceptarán su versión del registro, puesto que el contenido será distinto.

Estas tres propiedades son atribuibles de forma general a las redes blockchain. Sin embargo, existen otros parámetros que los desarrolladores tienen en cuenta y deciden a la hora de configurar estas redes, dependiendo de la función a la que cada red esté destinada, y que permiten matizar lo que acabamos de exponer. En particular, en función de las decisiones sobre algunos de estos parámetros, las redes blockchain pueden ser públicas o privadas:

- **Redes públicas:** no exigen a los usuarios el cumplimiento de ningún requisito para poder unirse a ellas (e.g., requisitos de identificación) y no existe ninguna jerarquía entre los nodos, por lo que cualquier nodo puede convertirse en nodo validador si lo desea. El contenido de la cadena de bloques es transparente y visible para todos los usuarios (en algunos casos, incluso para aquellos que no son usuarios de la red). Puesto que estas redes no exigen permiso o invitación alguna para poder acceder y participar, reciben el calificativo de permissionless.

  Para evitar el fraude, los nodos validadores, además de realizar las operaciones de validación, deben resolver un conjunto de problemas criptográficos antes de poder incorporar un nuevo bloque a la cadena de bloques (este tipo de sistema recibe el nombre de proof-of-work, como el ideado en su día por Nick Szabo). Puesto que para realizar estas tareas los nodos validadores deben poner a disposición de la red su poder computacional, con los gastos energéticos y a nivel de infraestructura que ello comporta[1], reciben una compensación por realizar esta tarea. En gran parte de las redes públicas, este incentivo se traduce en la recepción de una pequeña comisión al primer nodo validador que consigue resolver el problema criptográfico. Estos nodos validadores son también conocidos como «mineros» y su acción como «minar» o «minería».

- **Redes privadas:** un grupo limitado de actores conserva el poder de acceder, comprobar y añadir transacciones al libro registro. Este grupo también está en posición de decidir qué nuevos usuarios podrán incorporarse a la red y bajo qué requisitos (por ejemplo, tener relación laboral o de clientela con una determinada empresa, ser propietario de una determinada comunidad, pertenecer a un concreto grupo empresarial, etc.). Así, además, estas redes exigen el cumplimiento de determinados requisitos a aquellos usuarios que desean incorporarse a la red (e.g., identificación, procedimientos de KYC, etc.). Asimismo, también puede existir jerarquía entre los nodos, de modo que no cualquier usuario puede convertirse en un nodo validador o tener acceso a todos los datos sobre los usuarios. En este tipo de redes, los nodos validadores son nodos «de confianza» (en la acepción tradicional del término), esto es, entes en quienes todos los usuarios confían y que no necesitan ningún incentivo para realizar las tareas de validación (de modo que los «mineros» no son necesarios). En la terminología específica, el antes mencionado sistema proof-of-work se sustituye en estos casos por un sistema proof-of-stake o proof-of-authority. El

[1] Aunque en los inicios de las redes blockchain el minado podía realizarse mediante un ordenador corriente, la especialización y la profesionalización de los mineros es cada vez mayor (POP-PER, Nathaniel: «There Is Nothing Virtual About Bitcoin's Energy Appetite», The New York Times, 21 de enero de 2018, https://www.nytimes.com/2018/01/21/technology/bitcoin-mining-energy-consumption.html). La enorme exigencia energética de esta tecnología ha sido mencionada en muchas ocasiones como un factor determinante de su inviabilidad (BBC Mundo. Redacción: Por qué se gasta tanta electricidad para producir bitcoins (y qué tan cierto es que consume tanta energía como Dinamarca), 12 de diciembre de 2017, http://www.bbc.com/mundo/noticias-42323617).

proceso de validación de transacciones es más rápido que el de las redes públicas, a la vez que consume menos energía[2]. También se suele mantener que el encargo de la gestión solamente a participantes leales y la reducción de los procesos requeridos para su funcionamiento reducen igualmente el riesgo de sufrir ciberataques y brechas de seguridad. Por todo ello, estas redes reciben el calificativo de permissioned.

Aplicaciones

Con carácter general, habida cuenta de sus características, tal y como han quedado expuestas en el apartado anterior, la utilización de esta tecnología podría aportar valor añadido, teóricamente, a aquellas actividades que cumplan con las siguientes condiciones: (i) requieran almacenar datos, (ii) precisen que el acceso a estos datos sea compartido entre diferentes partes y (iii) estas partes no se conozcan entre ellas o no exista confianza mutua por otro motivo. Son muchas las actividades que se desarrollan o pueden desarrollarse bajo los anteriores parámetros, por lo que la utilización del blockchain se ha descrito, y se está desarrollando ya materialmente, en multitud de sectores y para un sinfín de aplicaciones. A continuación, se presentan algunas.

- **Criptomonedas:** El Banco Central Europeo definió ya en 2012 las «criptomonedas» o «monedas virtuales» como «un tipo de dinero digital y no regulado, normalmente emitido y controlado por sus desarrolladores, y usado y aceptado entre los miembros de una concreta comunidad virtual»[3]. Con posterioridad, en la recientemente aprobada Directiva del Parlamento Europeo y del Consejo por la que se modifica la Directiva (UE) 2015/849, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo[4], se definen las «monedas virtuales» como una «representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos»[5].

[2] ASTRI: «Whitepaper On Distributed Ledger Technology», Hong Kong Monetary Authority, 11 de noviembre de 2016, pág. 34, https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper$_{O}$n$_{D}$istributed$_{L}$edger$_{T}$echnology.pdf

[3] European Central Bank: Virtual Currency Schemes, octubre 2012, pág. 5, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[4] Aprobada el 26 de abril de 2018: http://data.consilium.europa.eu/doc/document/PE-72-2017-INIT/en/pdf

[5] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2018-0178+0+DOC+XML+V0//ES#BKMD-5

Hoy en día existen miles de criptomonedas, cientos de ellas son creadas cada semana, aunque las más extendidas son el bitcoin (BTC) y el ether (ETH). Las redes Bitcoin y Ethereum tienen elementos comunes, pero se diferencian en algunos aspectos:

- **Bitcoin:** Red creada en 2009. Está programada para finalizar la emisión de bitcoins cuando se alcance la cifra de 21 millones de BTC emitidos. La red Bitcoin está diseñada para funcionar como medio de pago entre aquellos que deciden voluntariamente aceptarlo como tal.
- **Ethereum:** Red creada en 2015 por Vitalik Buterin. Aunque la emisión de ethers es, en principio, ilimitada, la emisión anual está limitada a 18 millones de unidades. La principal diferencia con la red Bitcoin es que la red Ethereum permite realizar transacciones más sofisticadas que el mero pago, al admitir que operen sobre su estructura ciertos *smart contracts*, a los que nos referiremos más adelante.

- **ICO (Initial Coin Offerings) e ILP (Initial Loan Procurements):** Aunque originariamente fueron creados para funcionar como medio de pago, los activos virtuales rápidamente se convirtieron en valor de cambio de distintas contraprestaciones, incluyendo nuevos modos de captación de fondos de inversores para financiar futuros negocios. En este ámbito, los promotores de las llamadas ICO (Initial Coin Offering) ofrecen, a cambio de moneda de curso legal o moneda virtual, un token, una especie de vale virtual, instrumentado como apunte digital del derecho a la obtención de distintos beneficios posibles, como el acceso o posibilidad de adquisición de un producto o servicio todavía no lanzado al mercado (utility tokens), o, incluso, un interés participativo en los futuros ingresos o el posible aumento del valor de la entidad emisora o del negocio (equity tokens)[6].

  Al igual que las ICO, los recién surgidos ILP (Initial Loan Procurements) se están destinando a captar fondos para nuevos proyectos. En este caso, los usuarios que deciden acudir a la oferta reciben tokens de acceso a derechos de crédito transmisibles a terceros o FLATS (Future Loan Access Tokens). La aportación se articula a través de un contrato de préstamo con el receptor de los fondos en formato smart contract, código autoejecutable, en cuya virtud el prestador recibe los pagos de forma automática y sin la intervención de operador alguno[7].

[6] Comisión Nacional del Mercado de Valores: Comunicado difundido por la Securities and Exchange Commission con consideraciones de su presidente sobre las criptomonedas y las denominadas «ofertas iniciales de criptomonedas» («Initial Coin Offerings» o «ICOs»), enero de 2018, págs. 6 y 7, http://www.cnmv.es/portal/verDoc.axd?t=14a617e8-7f18-40e0-9f1b-2061d924f5f4

[7] SAYER, Luke: «Goodbye ICOs, hello ILPs?», Business Brief, 346, 2018, págs. 34-35.

- **Smart contracts:** Los denominados smart contracts o «contratos inteligentes», que se han mencionado ya al referirnos a las posibilidades técnicas de la red Ethereum y a la devolución automática al prestador en los ILP, se suelen describir como «contratos» autoejecutables. Si son o no contratos dependerá en cada caso de si concurren los requisitos de consentimiento, objeto y causa para ello. En cualquier caso, en rigor, la aptitud para ser jurídicamente contrato no corresponde a lo que comúnmente se conoce como smart contract, y que no es más que programa autoejecutable, sino a lo que se ha denominado «contrato legal inteligente», del que el smart contract es solo parte, y que se ha definido como el contrato celebrado «a través de una página web accesible para las partes cuya forma está constituida por la interfaz de usuario de la aplicación externa y uno o varios programas autoejecutables (smart contracts) residentes en la cadena de bloques con capacidad para actuar recíprocamente con dicha interfaz»[8].

Literatura en Blockchain

Se realizó una búsqueda y clasificación de la literatura relacionada a Blockchain en el sector financiero en la base de datos de Scopus[9]. Se hizo la revisión de 860 documentos y la clasificación de los 30 documentos más relevantes.

Concept \ Category	Computers and Society
Blockchain Architecture	[18] [15] [34] [40] [37][35][14][41][21][25][45][55][23][47][46]
System Framework	[18] [30] [53][14][55][47]
Cryptocurrencies	[34] [40][14][27][45][46]
Consensus Algorithm	[15] [37] [30] [40][53][14][41][21][25][55]
Future of Blockchain	[34] [40][53][35][21][25][27][45]

Cuadro 2.1: Estado del arte de Blockchain en el sector tecnológico

Concept \ Category	Electronic commerce
Blockchain Architecture	[51] [26] [42][10][7]
System Framework	[50][51] [26] [52] [42] [16] [22][3][12][9][17][10][28][7]
Cryptocurrencies	[51][26][52][42] [16][39][3][9][17][10]
Consensus Algorithm	[26] [42] [16] [22] [39][12][9][10][28]
Future of Blockchain	[51]

Cuadro 2.2: Estado del arte de Blockchain en el sector financiero

En base a la investigación anterior, Blockchain aún se considera una tecnología de innovación y no tiene un puesto establecido como una investigación dentro del área. Además, la mayor parte de la investigación previa se centra exclusivamente en aspectos de infraestructura tecnológica, como la seguridad, el anonimato, la escalabilidad o la flexibilidad de protocolos de consenso.

[8] TUR FAÚNDEZ, Carlos: Smart contracts, análisis jurídico, Editorial Reus, Madrid, 2018, pág. 60.
[9] https://www.scopus.com/home.uri

2.2. Bitcoin

Es una moneda digital y un sistema de pago en línea en el que se utilizan técnicas de encriptado para regular la generación de las unidades de moneda y verificar las transferencias de fondos, operando independientemente de una autoridad central. La terminología puede ser confusa porque las palabras Bitcoin y Blockchain se pueden utilizar para referirse a cualquiera de las tres partes del concepto: la tecnología de la cadena de bloques subyacente, el protocolo y el cliente a través del cual se realizan las transacciones, y a la criptomoneda en sí; o también más ampliamente para referirse a todo el concepto de las criptomonedas.

Bitcoin fue creado en 2009 por una persona o entidad desconocida bajo el seudónimo de Satoshi Nakamoto. El concepto y los detalles operativos son descritos en un informe técnico [32]. Los pagos se registran en un libro contable público y distribuido que se almacena en cada uno de los participantes de Bitcoin, conocidos como nodos, y que pueden verse continuamente a través de Internet. Bitcoin es la primera y más grande criptomoneda descentralizada.

Hay cientos de otras criptomonedas, denominadas "altcoin" (monedas alternativas), pero Bitcoin comprende el 50 % de la capitalización bursátil de todas las criptomonedas y es el estándar de facto. Bitcoin es seudónimo (no anónimo) en el sentido de que se utilizan direcciones de clave pública (cadenas de caracteres alfanuméricos; similar en función a una dirección de correo electrónico) para enviar y recibir Bitcoins y para registrar esas transacciones, por lo tanto, no se requiere la transmisión de información de identificación personal.

Los bitcoins son generados como una recompensa por la realización de un trabajo de procesamiento computacional, conocido como minería, en el que los usuarios de la red ofrecen su poder de cómputo para verificar y registrar las transacciones en la cadena de bloques. Los individuos o empresas participan en la minería a cambio de las comisiones por cada transacción y por Bitcoins recién generados.

Además de la minería, los bitcoins pueden, como cualquier moneda, obtenerse a cambio de dinero fiduciario, productos o servicios. Los usuarios pueden enviar y recibir bitcoins electrónicamente por una comisión de transacción opcional utilizando un software en una computadora personal, dispositivo móvil o aplicación web, que funcionan como billeteras.

Ventajas

El dinero es un medio de intercambio para el pago de bienes y servicios en la sociedad, tiene un valor contable. El valor del dinero tiene un componente regulatorio controlado por un organismo o entidad, que normalmente es un Banco Central, pero a la vez tiene un valor intrínseco de confianza otorgado por la sociedad que lo utiliza.

El Bitcoin se está convirtiendo en un refugio para algunos inversores, todavía pequeños, bastante experimentales, pero reales, debido a sus numerosas ventajas que incluyen:

- Tendrá un límite de emisión que llegará a 21 millones. Esto la convierte en una moneda que tiende a apreciarse frente a otras. El dólar perdió el 90 % de su valor en 50 años, como consecuencia de la creciente emisión, el Bitcoin garantiza que la emisión tendrá un tope.
- Una moneda con restricción de emisión se traduce en deflación de precios, es decir, un bien comprado hoy con Bitcoin sería más caro que si se compra más adelante, porque el valor de la moneda va hacia la apreciación.
- Es una moneda "anónima", no la puede controlar un gobierno, ni una entidad. En un punto se parece al sistema previo a la aparición de los Bancos Centrales, donde cada entidad respaldaba su dinero con sus propias reservas. Al no estar regulada por un organismo es menos manipulable, porque intervienen tantos actores que resulta imposible lograr que todos acuerden una acción común
- El control de las transacciones es realizado por todos los participantes del ecosistema Bitcoin, cada operación queda completamente registrada, de tal manera que cualquiera puede ver movimientos, aunque sin poder detectar quién los hace.
- Las transacciones se hacen en tiempo real. Cualquier transferencia de dinero de un país a otro suele demandar entre 24 y 72 horas. Esta moneda, se transfiere en tiempo real de una cuenta a otra.

Mejores prácticas

Bitcoin es una tecnología descentralizada bastante nueva que funciona de manera diferente a cualquier otro sistema de pagos que haya existido anteriormente. Sus usuarios deben tener cuidado al utilizar Bitcoin porque no existe una autoridad central que pueda proteger sus fondos o de revertir transacciones. Existen las denominadas "buenas prácticas" de Bitcoin que todo usuario debe tener en cuenta al entrar en este ecosistema.

Esta lista de buenas prácticas es no exhaustiva pero cubre la mayoría de los casos para proteger a los usuarios nuevos:

- **No permita que otros almacenen sus Bitcoin:** Muchos usuarios nuevos a Bitcoin tienen la costumbre de almacenar sus Bitcoin en billeteras en línea donde realizaron la compra de sus monedas. Esta es una muy mala idea por 2 razones:

  1. Los servicios de intercambio son expuestos a **ciberataques**[10].
  2. Los servicios de intercambio **huyen con las monedas** de sus usuarios todo el tiempo.

  Hay una regla que es muy importante recordar: Los Bitcoin le pertenecen únicamente al usuario que tenga la llave privada.

- **No invierta más de lo que está dispuesto a perder:** Bitcoin es una tecnología bastante nueva que apenas se está probando en escenarios del mundo real. Como cualquier otra nueva tecnología, podría despegar o podría fallar. Puede parecer una buena idea invertir todo lo que tiene porque la volatilidad demostrada de Bitcoin ha hecho que muchas personas se hagan muy ricas, pero también ha causado que muchas otras personas quiebren.

- **Tómese el tiempo de evaluar sus opciones de billeteras:** Hay muchas billeteras diferentes que van desde muy seguras hasta muy convenientes. Elegir la correcta es una decisión muy importante y depende el uso que el usuario pretenda darle a sus monedas.

- **Respalde su billetera:** Las computadoras y teléfonos móviles pueden averiarse o extraviarse en cualquier momento y, como resultado, se puede perder el acceso las monedas de manera permanente. Es necesario respaldar la llave privada para poder restaurar la billetera en cualquier momento en el futuro.

- **No reutilice direcciones Bitcoin:** Dado que Bitcoin no es anónimo y Blockchain es de acceso público, se recomienda encarecidamente no reutilizar las direcciones de billetera. Cuando se utiliza una dirección única para múltiples transacciones, se vinculan todas las transacciones futuras. Este vínculo se puede utilizar para analizar los pagos que puede comprometer la privacidad y seguridad del usuario. Por suerte, la mayoría de las billeteras generan nuevas direcciones cada que se recibe un pago.

[10] Explotación deliberada de sistemas informáticos, empresas y redes dependientes de la tecnología. Estos ataques utilizan códigos maliciosos para alterar la lógica o los datos del ordenador, lo que genera consecuencias perjudiciales que pueden comprometer información y provocar delitos cibernéticos, como el robo de identidad.

2.3. Sistemas PoS

Un sistema de PoS (por sus siglas en inglés, Point of Sale) o punto de venta en español, es un conjunto de herramientas de hardware y software, que principalmente le permiten a los negocios facturar sus ventas, facilitando también llevar el control de su flujo de caja, inventarios, proveedores, compras, cuentas por cobrar y pagar, gastos y costos fijos, utilidades y pérdidas, entre otras funciones.

Además, un sistema de POS puede ayudar a mejorar la atención al cliente en el punto de venta, disminuyendo su tiempo de espera, fidelizándolos con herramientas como puntos por compras, créditos directos, promociones por SMS, diversas formas de pago, etc.

Considerando el mercado global, se estima que el valor del software de los sistemas PoS aumente de $1.34 mil millones de dólares en 2018 a $3.73 mil millones en 2023 [36]. Este enfoque revolucionario ofrece nuevas perspectivas para los negocios minoristas en todo el mundo. Los mostradores de punto de venta modernos tienen un componente de software configurados en una computadora personal o dispositivos móviles que ejecutan programas basados en la nube, que luego se conectan a un componente de hardware de forma local, por medio de lectores de tarjetas y escáneres de códigos de barras.

Las soluciones PoS basados en la nube ayudan a las empresas a mejorar y manejar una amplia gama de opciones de pago. Son una herramienta vital para aumentar las ventas. También brindan soporte en precios y control de inventario, mercadotecnia, contabilidad, servicio al cliente y firmas digitales. Estas soluciones ayudan a las empresas a ahorrar en costos de propiedad y tiempos de implementación, así como simplifican la administración de un establecimiento.

Debido al alto número de soluciones de punto de venta disponibles, existen factores importantes a considerar al escoger un sistema de este tipo:

- **Integraciones**: El sistema debe poder integrarse no solo con su software comercial actual, sino también con aplicaciones relacionadas de terceros que se puedan considerar en el futuro o que proporcionen funcionalidad adicional.
- **Procesamiento de pagos**: El sistema debe ser capaz de soportar una amplia gama de opciones de pago y procesadores de pago.
- **Facilidad de uso**: El sistema no debe requerir habilidades técnicas avanzadas. Incluso usuarios sin conocimiento técnico deben ser capaces de instalar y operar el sistema sin ninguna dificultad.

- **Gestión de inventario**: El sistema debe soportar algún tipo de manejo de inventario; esto incluye controlar disponibilidad, configurar promociones y manejar descuentos, además de facilitar el seguimiento en tiempo real de los productos disponibles.

En general, el proceso de selección para un sistema PoS debe guiarse fundamentalmente por las necesidades de cada negocio. Existen varios sistemas de punto de venta que ofrecen una experiencia integral en el procesamiento de pagos y que se encuentran establecidos en la industria. Entre ellos se incluyen:

- **Shopify**

  Shopify[11] es esencialmente una plataforma de comercio electrónico que proporciona capacidades de punto de venta adicionales. Sin embargo, este servicio se centra fundamentalmente en las características de una tienda en línea, y se aplica mejor a negocios que venden principalmente en línea mientras administran tiendas minoristas secundarias.

- **Square POS**

  Square POS[12] es ideal para nuevas o pequeñas empresas con un presupuesto limitado. Los pequeños restaurantes y minoristas puede hacer uso de sus propias aplicaciones especializadas que se adaptan a sus necesidades.

- **Airpos POS**

  El sistema Airpos POS[13] logra simplificar el proceso de un punto de venta en la nube, especialmente para pequeños negocios. Proporciona características básicas pero flexibles a un precio accesible, además de capacidades de comercio electrónico complementarias gratuitas. Este sistema es adecuado para las pequeñas y medianas empresas que tienen la intención de vender en múltiples ubicaciones físicas, que son complementadas por tiendas en línea.

- **Aspel**

  Aspel CAJA[14] controla, administra y agiliza las operaciones de ventas, facturación e inventarios de uno o varios comercios, convirtiendo una computadora en un punto de venta capaz de operar con impresoras de tickets, cajas, básculas, lectores ópticos de código de barras, lectores de tarjetas de crédito y pantallas táctiles.

[11] https://www.shopify.com/pos
[12] https://squareup.com/us/en/point-of-sale
[13] https://www.airpointofsale.com/
[14] https://www.aspel.com.mx/

- **ManagementPro**

  ManagementPro POS[15] es un sistema PoS diseñado para negocios con atención al público que requieran agilidad máxima en su operación. Esta herramienta registra las ventas, controla inventarios, facturaciones y más. Cuenta con una interfaz amigable y fácil de usar, un diseño intuitivo para mejorar la experiencia del usuario. Ofrece un kit completo para PoS para sus usuarios.

- **ContPaqi**

  ContPaqi[16] es un sistema que integra de manera ágil las operaciones en un punto de venta diseñado para empresas de comercio al detalle que requieren control de su caja e inventarios.

- **SICAR**

  SICAR[17] Punto de Venta es un software que ayuda a vender de una forma sencilla, con una interfaz fácil y con la rapidez que una empresa necesita, SICAR ayuda a controlar las entradas y salidas de dinero, así como las compras, ventas, inventarios, créditos, cuentas por pagar, cuentas por cobrar, facturación electrónica, venta de recargas electrónicas, control de sucursales, etc.

2.4. Pagos en Blockchain

Por lo que se sabe, no se ha puesto suficiente atención por parte de la comunidad académica a las terminales de punto de venta (PoS) de Bitcoin (o cualquier otra criptomoneda), y a sus requerimientos en términos de seguridad, usabilidad e implementabilidad. La mayoría de los sistemas de pago existentes se adaptan a los mercados en línea (e.g., e-commerce) y no a los puntos de venta físicos [8]. A continuación se enlistan los enfoques disponibles para aceptar pagos de Bitcoin que se pueden adaptar para transacciones en punto de venta.

- **Dirección Bitcoin en mostrador**

  Una forma sencilla de acepar Bitcoin es generar una dirección pública de Bitcoin utilizando cualquier billetera digital y mostrarla en mostrador para que los clientes pueden escanearla utilizando, por ejemplo, un código QR. Cualquier cliente puede escanear este código (utilizando cualquier billetera móvil para Bitcoin) e ingresar el monto a pagar de forma fluida.

[15] https://www.mproerp.com/
[16] https://www.contpaqi.com/CONTPAQi/
[17] https://www.sicar.mx/punto-de-venta/

- **Terminales de hardware**

  Hay varias propuestas de terminales de hardware para aceptar Bitcoin[18], sin embargo, debido al alto costo de ejecución (por ejemplo, BATMFour se vende al precio inicial de $6499USD), no se utilizan en la mayoría de las pequeñas empresas y no se les ha hecho una revisión previa. El futuro de los terminales de hardware de Bitcoin es indeterminado.

- **Terminales de venta en línea**

  La mayoría de estos servicios no tienen una implementación explícita para un sistema de pago en punto de venta. Dos de los más populares son Bitpay[19] (0 % de comisión) y Coinbase[20] (1 % de comisión en el intercambio de Bitcoin-fiat).

- **Mycelium Gear**

  Mycelium Gear[21] es un servicio ofrecido por Mycelium que ofrece un widget como interfaz para el usuario y un servicio que utiliza una llave pública de tipo BIP32[22] [49] provista por un panel de administración para generar nuevas direcciones de manera segura. Esto significa que ellos no mantienen ninguna llave privada, pero utilizan el mismo conjunto de rutas para generar las direcciones que utiliza su billetera móvil "*Mycelium*"[23].

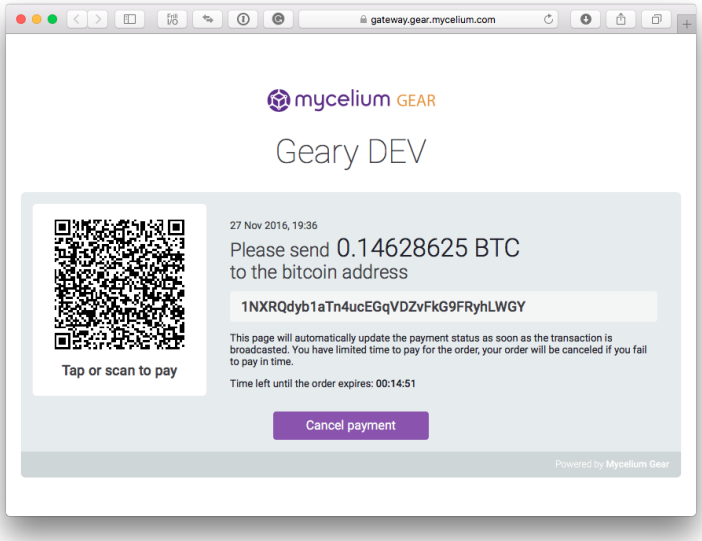


FIGURA 2.3: Widget de Mycelium Gear

[18] BATMFour (https://www.generalbytes.com/en/products/batmfour/), Revel Systems (https://revelsystems.com/pos-systems/), Coinkite (https://coinkite.com/)
[19] https://bitpay.com/
[20] https://www.coinbase.com/
[21] https://gear.mycelium.com/
[22] Billeteras deterministas jerárquicas
[23] https://wallet.mycelium.com/

- **Proyectos de la comunidad**

  La idea de terminales en punto de venta que utilicen Blockchain no es nueva. Existen múltiples pruebas de concepto e implementaciones propuestas por la comunidad que pretenden unir la idea de pagos en Blockchain con terminales en punto de venta. La mayoría de estas pruebas de concepto sirven como una demostración de lo que podría lograrse con estos sistemas y contienen documentación limitada o nula, por lo tanto no están destinadas a ser utilizadas en el mundo real y requieren el diseño de alguna infraestructura que soporte su implementación. Algunas propuestas destacadas incluyen:

  - **Blockchain Android Merchant App**

    Solución ideal de punto de venta (POS) desarrollada para dispositivos Android enfocada a restaurantes, bares, cafeterías y muchos otros comercios minoristas para aceptar pagos en Bitcoin. Implementa su propia API[24] para obtener precios y generar direcciones Bitcoin.

  - **GreenAddress POS**

    Está pensado para utilizarse en una PC estándar (utilizada por el comerciante) con un monitor externo (frente al cliente). El modo principal de operación es mostrar un código QR con una URI[25] del pago al cliente. Pero el software también admite el uso de la tecnología NFC[26] para transmitir el URI a través de Bluetooth.

  - **Pyxpub**

    Es un software de código abierto que genera solicitudes de pago únicas en Bitcoin sin terceros involucrados. Los costos de ejecución son limitados al dispositivo (computadora personal o móvil) y una conexión a Internet. Expone las características necesarias para la recepción de pagos locales a través de una API que permite el desarrollo de un sistemas de punto de venta. Esta aplicación facilita el seguimiento de las mejores prácticas de Bitcoin y permite escalar la aplicación a cualquier necesidad futura.

[24] Una API (siglas de 'Application Programming Interface') es un conjunto de reglas (código) y especificaciones que las aplicaciones pueden seguir para comunicarse entre ellas: sirviendo de interfaz entre programas diferentes de la misma manera en que la interfaz de usuario facilita la interacción humano-software.

[25] URI son las siglas en inglés de Uniform Resource Identifier (en español identificador uniforme de recursos), que sirve para identificar recursos en Internet, precisamente lo que el nombre indica. Dicho identificador de recursos tiene un formato estándar definido y su propósito es permitir interacción entre recursos disponibles en Internet, o en alguna red de cómputo. La información transmitida dentro de este contexto puede incluir una dirección Bitcoin a dónde enviar un pago y el monto requerido.

[26] Se trata de una tecnología inalámbrica de alta frecuencia que se basa en la creación de un campo electromagnético en el que, mediante inducción, se genera un intercambio de información entre ambos dispositivos.

2.5. Exchange

Un "Exchange" es una plataforma de intercambio de activos, para fines modernos esta plataforma es electrónica o digital, y para fines aún más modernos, los activos que se pueden intercambiar también son digitales. El servicio que ofrece es empatar a compradores y vendedores a través de la plataforma. Todos los "exchanges" tienen diferentes precios entre ellos. Es parte de su naturaleza al ser plataformas de intercambio libre. Esto es así dado que todos los usuarios generan "posturas de compraventa" en la plataforma, a la lista de posturas de compra y venta de los activos se le llama "libro de órdenes" (*order book* en inglés). La plataforma simplemente lo que hace es que cuando el precio de compra de una orden empata con el precio de venta de otra para determinado activo, ejecuta un intercambio o "trade" en inglés. Por esta misma razón, los demás "exchanges" generan ganancias por las comisiones de cada transacción y no por el precio del activo cotizado, es un tipo de "casa de cambio" donde los que intercambian lo hacen directamente con la casa, quien define un precio de compra y otro de venta.

FIGURA 2.4: Libro de órdenes (Order book)

Ejemplos de exchanges son:

- **New York Stock Exchange**

  Bolsa de Valores o Sitio de intercambio de activos, es el sitio con mayor capitalización a nivel mundial e intercambia principalmente acciones, bonos de deuda y ETFs[27].

[27] Un ETF (Exchange-traded funds) es un conjunto de activos que cotiza en la bolsa de valores. Los ETFs son vehículos que ayudan a invertir de manera diversificada y con bajo costo.

- **Nasdaq**

  Plataforma de intercambio de activos, la segunda más grande en términos de capitalización mundial. Entre las clases de activos disponibles están: Acciones, "commodities" (materias primas) y derivados.

- **Chicago Mercantile Exchange**

  Exchange o plataforma de intercambio de activos. Principalmente permite intercambiar materias primas y derivados asociados a éstas.

- **Bolsa Mexicana de Valores**

  Sitio de intercambio de activos en México. Principalmente permite intercambiar acciones y bonos de deuda nacional.

- **MEXDER**

  Sitio de intercambio de derivados en México como Futuros[28], Opciones[29] y Swaps[30].

- **Bitso**

  Sitio de intercambio de divisas digitales y peso mexicano. Permite intercambiar monedas digitales como Bitcoin, Ether y XRP por moneda nacional.

[28]Un contrato de futuros es un contrato o acuerdo que obliga a las partes contratantes a comprar o vender un número determinado de bienes o valores (activo subyacente) en una fecha futura y determinada, y con un precio establecido de antemano.

[29]Las opciones financieras son instrumentos financieros que otorgan al comprador el derecho y al vendedor la obligación de realizar la transacción a un precio fijado y en una fecha determinada.

[30]Un 'swap' es un acuerdo de intercambio financiero en el que una de las partes se compromete a pagar con una cierta periodicidad una serie de flujos monetarios a cambio de recibir otra serie de flujos de la otra parte. Estos flujos responden normalmente a un pago de intereses sobre el nominal del 'swap'.

3 Desarrollo

3.1. Marco de evaluación

Se propone un marco para comparar las diversas soluciones PoS de Bitcoin disponibles, clasificando estos sistemas en usabilidad, aplicabilidad, privacidad y seguridad [5]. Estos no son un conjunto completo de requisitos para un sistema de punto de venta de propósito general, pero están diseñados para un volumen bajo de transacciones en persona que se pudieran encontrar en una PyME[1]. Estos requerimientos se utilizan para calificar cada sistema en la Figura 4.1. Para simplificar la figura, utilizamos tres indicadores de puntaje. (•) para obtener una puntuación completa del requisito, (o) si los requisitos no se han cumplido por completo y el espacio vacío si no satisface la necesidad. Para algunos de los requisitos, el sistema de puntuación puede no ser intuitivo (por ejemplo, bajo costo de ejecución), sin embargo, se justifica cada puntaje más adelante en el documento.

- **USABILIDAD**

  Se consideran los siguientes aspectos de usabilidad.

  - **Facilidad de uso**: esta es una categoría que denota cualquier falla en la usabilidad que resulte en un proceso demasiado técnico o complejo para el empleado o cliente. Una sola sesión de capacitación para el empleado debería ser suficiente y el sistema debería ser intuitivo para cualquier usuario de Bitcoin. Debe haber una comprensión clara y mutua cuando se finaliza un pago. Un punto de venta que tenga todas estas características se puntuaría (•), mientras que tener algunas resultaría (o).
  - **Eficiencia**: el procesamiento de los pagos no debería demorar mucho más tiempo que los sistemas de pago comunes, como los pagos con tarjeta de crédito/débito. Si el proceso toma el mismo tiempo que los pagos con tarjeta de crédito, se obtendría un puntaje (•), cualquier cosa más que eso sería (o) o ninguno.

[1] Pequeña y mediana empresa

- **Tipo de cambio justo**: debe haber una forma fácil y verificable de llegar a un acuerdo entre el cliente y el negocio acerca del tipo de cambio, de dinero fiat[2] a Bitcoin, a utilizar. Si el precio se obtiene de fuentes comúnmente aceptadas, se puntuaría (•).
- **Disponibilidad**: todos los empleados deben poder realizar el proceso de pago de Bitcoin sin necesidad de conocer ningún tipo de credenciales. Si la aplicación se encuentra en un dominio público para que cualquiera pueda acceder, se puntuará (•), si necesita información privada se puntuará (o) y si necesita credenciales no se puntuará.

- **APLICABILIDAD**

  Esta categoría indica los requisitos con respecto a la implementación.

  - **Bajo costo de ejecución**: El PoS debe ser accesible con algún dispositivo electrónico perteneciente al negocio, como la computadora del cajero, alguna terminal PoS[3] o un dispositivo móvil. No debería haber necesidad de comprar nuevo hardware o software costoso. Para este requisito, obtendríamos un puntaje (•) en un sistema libre de costos monetarios y un puntaje (o) en una cantidad moderada de gastos.
  - **Habilita la ramificación**: La capacidad de instalar el punto de venta de forma sincronizada en múltiples establecimientos del negocio. Puede ser necesaria alguna configuración para diferenciar dos ramas diferentes en el sistema. Si el sistema se encuentra empaquetado y es fácil de instalar en algún otro establecimiento de la empresa, obtendrá una puntuación (•), si necesita alguna modificación (o) y si es el mismo procedimiento para instalarlo que el primero, no obtendrá ninguna.
  - **Permite la conversión de divisas simultánea**: Debe ser posible al negocio recibir sus pagos en la divisa que desee. Esto incluye dinero fiat o cualquier criptomoneda que se haya configurado. Si el sistema permite configurar la salida de pagos con dinero fiat (haciendo la conversión instantánea al momento de recibir un pago), se obtendrá una puntuación (•).

- **PRIVACIDAD**

  Como las transacciones en Bitcoin se registran por medio de Blockchain, es importante considerar la privacidad tanto del cliente como del negocio.

  - **Sin pérdida de información**: no debe haber información confidencial o sensible disponible al cliente al momento de pagar con Bitcoin. Esta información

[2] Dinero emitido por el gobierno
[3] El más común siendo las terminales de tarjetas de crédito/débito

puede incluir la infraestructura de la red de la empresa o un dominio privado utilizado para fines contables. Si se filtra información confidencial, no se puntuará y si se filtra información no confidencial se puntuará (o).

- **Mantiene la privacidad del negocio**: el cliente no debería poder ver cuánto ha recibido el negocio antes o después de su pago, sino solo su propio monto del pago actual. Si no hay un vínculo entre los pagos por un cliente, el PoS puntuará (•).
- **Mantiene la privacidad del cliente**: el negocio no debería poder ver cuánto posee el cliente, ni su historial de transacciones. Este tema aún no se resuelve por completo[2]. Todos los sistemas en esta evaluación obtuvieron un puntaje (o), incluido el desarrollado en este documento, se incluye esta propiedad para tener un marco completo para la evaluación de software futuro que pueda utilizar complementos que preserven la privacidad[6] o criptomonedas [29].
- **Lista de pagos confidenciales**: la capacidad de ver la lista de pagos, solo disponible para el administrador mediante un método de autenticación, como un panel protegido por contraseña. Si el sistema ofrece una página de informe para el gerente, se puntuará (o), si la página de informe podría tener autenticación jerárquica para los empleados con acceso limitado, se puntuará (•).

- **SEGURIDAD**

  La seguridad es uno de los aspectos más importantes de cualquier sistema de pago financiero. La seguridad del sistema representa algo más que su código, incluye el entorno en el que se está utilizando, las personas que usan el software y el entorno operativo del software.

  - **Sin confianza a terceros**: debe haber la menor cantidad de interacción posible con terceros para aceptar y mantener Bitcoin. La confianza total en un tercero dará como resultado una puntuación nula, algo de confianza en la funcionalidad principal del sistema en (o) y ninguna confianza dará como resultado una puntuación (•).
  - **Cifrado de datos**: en el caso de cualquier ataque al servicio, debe haber medidas de seguridad que aseguren que el atacante no podrá tener acceso a las claves privadas ni a transferir fondos de Bitcoin. Solo si todos los datos confidenciales están encriptados, el PoS puntuará (•).
  - **Sin dependencia de software**: el sistema debe usar la menor cantidad de dependencias posibles para minimizar el vector de ataque en el servidor. Si el sistema necesita un conjunto complejo de software o hardware para funcionar,

no obtendrá ninguna puntuación, y si se puede ejecutar en un navegador[4] sin la necesidad de ejecutar ningún otro software, obtendrá una puntuación (•).

3.2. Evaluación de las propuestas actuales

La mayoría de los sistemas de pago existentes se adaptan a los mercados en línea (por ejemplo, e-commerce) y no a puntos de venta físicos[5]. A continuación, se enumeran todos los enfoques disponibles para aceptar pagos de Bitcoin que al menos se podrían adaptar para transacciones en persona.

A. **Dirección Bitcoin en mostrador**

Una forma sencilla para que las pequeñas empresas acepten Bitcoin es generar una dirección de Bitcoin y mostrarla, como un código QR por ejemplo. Los clientes pueden escanear el código QR e ingresar el valor en su billetera Bitcoin y pagar a la empresa con los Bitcoins equivalentes.

a. **Usabilidad**

Este enfoque coloca al empleado en una posición donde tiene que preparase para recibir y verificar los pagos de Bitcoin manualmente (Facilidad de uso: ninguno). Esto hace que el tiempo dedicado al pago sea más largo que un sistema de pago integrado (Eficiencia: ninguno). La conversión de precios de la moneda local a BTC también sería una búsqueda manual (Tipo de cambio justo: ninguno). Se requiere capacitación técnica para cada empleado responsable de manejar los pagos de Bitcoin. Mientras la impresión del código QR se encuentre siempre visible al cliente, éste podrá pagar por su orden (Disponibilidad: •).

b. **Aplicabilidad**

El costo para implementar este método es casi cero (Bajo costo de ejecución: •). En caso de que haya múltiples sucursales, basta con más impresiones para tener múltiples puntos de venta (Habilita la ramificación: o). Debido a que es una dirección fija que se encuentra desplegada en el mostrador, no permite el intercambio de dinero fiat a crypto en cualquier forma (Permite la conversión de divisas simultánea: ninguno).

c. **Privacidad**

[4]Para usar un software PoS, se necesita un dispositivo móvil o una computadora y asumimos que un navegador web está instalado de forma predeterminada en estos dispositivos.

[5]https://en.bitcoin.it/wiki/How_to_accept_Bitcoin,_for_small_businesses

Este método no proporciona privacidad para la empresa (Mantiene la privacidad del negocio: ninguna). Como todas las transacciones de Bitcoin están disponibles públicamente en Blockchain, cualquier persona con conocimiento de la dirección de Bitcoin podría ver todos los pagos recibidos, por lo que cualquiera podría tener acceso al historial de transacciones, así como ver todas las direcciones emisoras de esos pagos (Mantiene la privacidad del cliente: o, Lista de pagos confidenciales: ninguno).

d. **Seguridad**

Aparte del sistema, el cual mantiene la llave privada, la seguridad no aplica en este enfoque (Sin confianza de terceros: •). La clave privada debe guardarse en un lugar seguro, a menos que los fondos se transfieran a otra dirección (por ejemplo, a cambio de efectivo). No hay software o datos involucrados, por lo tanto, no hay dependencia del software (Cifrado de datos: ninguno, Sin dependencia del software: •).

B. **Terminales de hardware**

Se han propuesto múltiples terminales de hardware para aceptar pagos en Bitcoin, sin embargo, el futuro de los terminales de hardware de Bitcoin es indeterminado actualmente.

a. **Usabilidad**

Las interfaces de cada una de estas propuestas son diferentes, pero sigue un patrón similar a un punto de venta ordinario que se utiliza por las compañías de tarjetas de crédito. Sin embargo, introducir un dispositivo nuevo al proceso de pago reduce la facilidad de uso y presenta la necesidad de entrenar a los empleados (Facilidad de uso: o). El tiempo y disponibilidad del pago a través de una terminal de hardware deber ser muy similar al de pagos con tarjetas de crédito, si no es que menor (Eficiencia: •). El cliente ni el negocio tienen ningún control sobre el tipo de cambio y es proporcionado por el sistema (Tipo de cambio justo: o). El dispositivo es accesible para cualquier persona que tenga acceso a los otros terminales de pago (Disponibilidad: •).

b. **Aplicabilidad**

Las terminales de hardware presentan un alto costo de implementación (Bajo costo de ejecución: ninguno). Además, en caso de presentarse múltiples establecimientos del negocio, se debe comprar una terminal para cada sucursal y esto hace que los costos sean aún más altos (Habilita la ramificación: ninguno). Algunos sistemas de hardware permiten configurar las salidas de pago en el sentido de los montos a retirar o de configurar retiros automáticos por intervalos de tiempo. Sin embargo, no se toca el tema de la conversión de dinero

fiat-crypto como forma de retiro (Permite la conversión de divisas simultánea: o).

c. **Privacidad**

Un pago en una terminal de hardware presenta la misma privacidad que las terminales de tarjetas de crédito normales, sin embargo, la privacidad del negocio depende de la implementación del sistema de pago (Mantiene la privacidad del negocio: •, Mantiene la privacidad del cliente: •). Las terminales también ofrecen una interfaz similar a las terminales de tarjetas de crédito al mostrar los pagos (Lista de pagos confidenciales: •).

d. **Seguridad**

El negocio no tiene control sobre sus claves privadas ni posee los fondos recibidos (Sin confianza a terceros: ninguno), por lo tanto, debe confiar en la compañía que proporciona las terminales para mantener los fondos seguros, y recibirá los pagos a plazos acordados con posibles comisiones. En cuanto a otros aspectos de seguridad, se asume que la implementación del sistema mantiene las claves privadas encriptadas y seguras (Cifrado de datos: •). Existen otros riesgos de seguridad al añadir un nuevo hardware o software a la computadora del cajero que quedan fuera del alcance de este documento (Sin dependencia del software: ninguno).

C. **Servicios comerciales en línea**

La mayoría de estos servicios no tienen una implementación explícita para un sistema de pago físico. Dos populares son Bitpay[6] (tarifas del 0 %) y Coinbase[7] (1 % en el intercambio de Bitcoins por dinero fiat).

a. **Usabilidad**

Implementar un pago en Bitpay es sencillo y fácil de implementar. No hay muchas opciones técnicas para el empleado (Facilidad de uso: •) y sus interfaces permiten la recepción de pagos de manera sencilla (Eficiencia: •). Tienen su propio tipo de cambio (Tipo de cambio justo: o) que el negocio puede establecer para convertir en efectivo tan pronto reciba los pagos, esto elimina el posible efecto que la volatilidad de los precios de Bitcoin podría tener en los pagos. Requiere algunas credenciales para acceder a la página del punto de venta (Disponibilidad: o).

b. **Aplicabilidad**

Lo único que requiere este requerimiento es un teléfono inteligente (smartphone) o una computadora pequeña con la que los usuarios puedan interactuar

[6] https://bitpay.com/
[7] https://coinbase.com/

y navegar a la pantalla de pagos, preferiblemente con una pantalla táctil para facilitar la entrada de precios e interacción del usuario (Bajo costo de ejecución: •). Es muy fácil agregar más sucursales a la cuenta original o incluso crear una nueva cuenta para la segunda sucursal (Habilita la ramificación: •). La meta principal de los servicios web es de agilizar la recepción de pagos en el área de e-commerce, por lo tanto, la mayoría cuenta con alguna integración con instituciones financieras para permitir el retiro de fiat directamente a las cuentas de banco del comerciante. Sin embargo, éstas transacciones pueden incurrir comisiones adicionales al servicio base, sin mencionar tiempos largos de retiro y opciones geográficas limitadas (Permite la conversión de divisas simultánea: o).

c. **Privacidad**

Bitpay tiene otro enfoque para preservar la privacidad. A medida que se generan nuevas direcciones para cada transacción, la privacidad del negocio y cliente se mantiene segura (Mantiene la privacidad del negocio: •, Mantiene la privacidad del cliente: •). Sin embargo, ha habido reportes de suspensiones de cuentas debido a pagos provenientes de direcciones Bitcoin sospechosas (ej. mercados negros[8] o LocalBitcoins[9]). En este caso, la privacidad, en el sentido que se está evaluando, se mantiene, pero quizás no en todos los aspectos necesarios en un sistema de pago. Para ver los pagos, el propietario del negocio debe iniciar sesión en la plataforma, pero otros empleados no pueden verlos utilizando ninguna otra cuenta (Lista de pagos confidenciales: o)

d. **Seguridad**

Bitpay ofrece uno de los sistemas de pago más seguros hasta el momento y no se han registrado ataques cibernéticos grandes (Cifrado de datos: o). Sin embargo, el usuario no tiene control sobre sus claves privadas y todas las claves son almacenadas en servidores de Bitpay (Sin confianza a terceros: ninguno), lo que significa una confianza completa a terceros. Debido a que son una solución basada en web, cualquier dispositivo con un navegador es suficiente para utilizar el punto de venta (Sin dependencia de software: •).

D. **Mycelium Gear**

Mycelium Gear[10] es un servicio ofrecido por el grupo Mycelium que ofrece un widget como interfaz para el usuario y un servicio que utiliza una clave pública BIP3214 [48] provista en un panel de administración para generar nuevas direcciones de forma segura. Esto significa que no mantienen ninguna clave privada. De igual

[8] https://es.wikipedia.org/wiki/Darknet
[9] Sitio de intercambio de Bitcoin https://localbitcoins.com/
[10] https://gear.mycelium.com/

manera, utilizan el mismo conjunto de rutas para la generación de direcciones que usa su billetera Mycelium Mobile.

a. **Usabilidad**

Mycelium Gear está diseñado para negocios de comercio electrónico y debe ser personalizado para adaptarse a un punto de venta en negocios físicos (Facilidad de uso: o). No hay comisiones relacionadas con el uso de este servicio, y se ofrecen verificaciones rápidas con soporte a transacción de 0 confirmaciones (Eficiencia: •) y es posible escoger de una lista de servicios de intercambio para obtener la tasa de cambio (Tipo de cambio justo: o). Se necesita una URL única para acceder a la página de pagos y los empleados deben conocer este enlace (Disponibilidad: o).

b. **Aplicabilidad**

El sistema debería ser fácil de implementar, pero de alguna manera resulta complicada la personalización ya no existe acceso al código para habilitar la configuración según las necesidades comerciales. El costo de ejecución dependiendo de la implementación podría ser casi cero (Bajo costo de ejecución: o). El único inconveniente de la implementación es que el negocio se ve forzado a utilizar la billetera de Mycelium Mobile para administrar sus pagos, sin embargo, al hacerlo, resulta fácil utilizar el sistema en otras sucursales y dedicar diferentes cuentas a cada sucursal (Habilita la ramificación: •). Por el momento no permite el retiro de fiat desde la aplicación (Permite la conversión de divisas simultánea: ninguno)

c. **Privacidad**

Como Mycelium Gear utiliza el protocolo BIP32 para generar direcciones Bitcoin para cada transacción, se mantiene la privacidad de ambas partes (Mantiene la privacidad del negocio: •, Mantiene la privacidad del cliente: •). Sin embargo, no existe soporte para la administración de usuarios para las pantallas de reporte. Si el cliente cierra la pantalla de pago exitosa, el empleado no puede verificar si el pago fue recibido o no, a menos que tengo acceso a la cuenta del administrador para verificar la lista de transacciones (Lista de pagos confidenciales: o).

d. **Seguridad**

Nada relacionado con el sistema PoS contiene información privada o claves que puedan estar en peligro de exposición, sin embargo, todos los demás aspectos del sistema se ejecutan dentro de la infraestructura de la aplicación (Sin confianza a terceros: o). Aunque todas las claves privadas se encuentran dentro de la billetera Mycelium (Sin dependencia de software: o), siempre existe el riesgo de malwares móviles o fallas de hardware (Cifrado de datos: o).

E. **Pyxpub**

Pyxpub[11] es un software de código abierto que genera solicitudes de pago únicas en Bitcoin sin terceros involucrados. Los costos de ejecución son limitados al dispositivo (computadora personal o móvil) y una conexión a Internet. Expone las características necesarias para la recepción de pagos locales a través de una API que permite el desarrollo de un sistemas de punto de venta. Esta aplicación facilita el seguimiento de las mejores prácticas de Bitcoin y permite escalar la aplicación a cualquier necesidad futura.

a. **Usabilidad**

Pyxpub tiene una interfaz minimalista que permite la rápida configuración de parámetros del negocio y de opciones de pago, como descuentos o impuestos. La interfaz también incluye una terminal que permite ingresar el monto a cobrar para generar códigos QR que un cliente puede escanear para realizar el pago (Facilidad de uso: •). Las tasas de conversión son obtenidas de múltiples fuentes configurables por el negocio (Tipo de cambio justo: •). Se realiza un seguimiento de cada petición de pago para indicar si se ha realizado un pago o no (Eficiencia: •). La aplicación no requiere credenciales para su uso (Disponibilidad: •).

b. **Aplicabilidad**

El sistema puede configurarse de forma local, en un computador personal o dispositivo móvil, o en un servidor web para acceso remoto y no requiere de equipo especial para su uso. Por su naturaleza, se puede configurar en distintos establecimientos de un negocio de manera individual o unificar todas las instancias para llevar un mejor control (Bajo costo de ejecución: •, Habilita la ramificación: •). Los pagos recibidos son enviados directamente al negocio, por medio de una llave pública previamente configurada. Sin embargo, no es posible la conversión de divisas a dinero fiat (Permite la conversión de divisas simultánea: ninguno).

c. **Privacidad**

La única información requerida para el funcionamiento del sistema es una llave pública (obtenida de cualquier billetera Bitcoin disponible) para usar como base en la generación de direcciones para la recepción de pagos. Se genera una nueva dirección Bitcoin para cada solicitud de pago para mantener la privacidad de ambas partes (Mantiene la privacidad del negocio: •, Mantiene la privacidad del cliente: •). Todas las solicitudes de pago son almacenadas en una base de datos para su acceso posterior. Debido a la naturaleza de

[11] https://pyxpub.io/

Blockchain, estas transacciones no contienen información del negocio o del cliente a cual se pueda vincular. (Lista de pagos confidenciales: •).

d. **Seguridad**

Al seguir los estándares y las mejores prácticas de Bitcoin, Pyxpub ofrece a sus usuarios a manejar los pagos de manera privada y segura. Una base única de código que se encarga de todas las partes críticas del sistema (Sin dependencia de software: •). Esto asegura la completa propiedad de las direcciones de pago y del flujo de estos pagos, así como la completa privacidad y facilidad de operación (Sin confianza a terceros: •). El sistema no maneja llaves privadas, por lo tanto, no tiene acceso a los pagos recibidos (Cifrado de datos: •).

Categoría	Facilidad de uso	Eficiencia	Tipo de cambio justo	Disponibilidad	Bajo costo de ejecución	Habilita la ramificación	Conversión de divisas simultánea	Mantiene la privacidad del negocio	Mantiene la privacidad del cliente	Lista de pagos confidenciales	Sin confianza a terceros	Cifrado de datos	Sin dependencia de software
Dirección Bitcoin en mostrador				•	•	◦			◦		•		•
Terminales de hardware	◦	•	◦	•				•	•	•		•	
Servicios comerciales en línea	•	•	◦	◦	•	•		•	•	◦		◦	•
Mycelium Gear	◦	•	◦	◦	◦	•		•	•	◦	◦	◦	◦
Pyxpub	•	•	•	•	•	•		•	•	•	•	•	•

FIGURA 3.1: Comparación de pasarelas de pagos en punto de venta

3.3. Diseño e implementación

Hay múltiples enfoques evidentes que pueden utilizarse para la implementación del sistema PoS. Uno de los métodos de menor costo sería utilizar una computadora conectada a la red del negocio como servidor web local, sin embargo, el mantenimiento y soporte podrían resultar una tarea difícil. La red puede verse saturada por la gran cantidad de dispositivos conectados a ella y puede que afecte el funcionamiento. El tiempo de funcionamiento (uptime) es uno de los aspectos más importantes para un sistema de pagos. La siguiente mejor solución de bajo costo es utilizar un servidor de alojamiento compartido para alojar la aplicación (servidor de la billetera, servidor para la tasa de intercambio, etc.) y diseñar una interfaz de pago basada en web que se comunique a este servidor y a cuál los empleados tienen acceso.

A. *Medidas de implementación*

1) Usabilidad

a. **Facilidad de uso (●):** La interfaz debe ser mínima y simple, con la capacidad de mostrar el tipo de cambio de Bitcoin a fiat, con pantallas de entrada en pesos mexicanos, estimaciones de los montos de Bitcoin equivalente al precio y una sección de notas. En cuanto a la interfaz de usuario, debe ser simple, mostrando toda la información requerida, como la cantidad en Bitcoin, el tipo de cambio y el código QR para recibir el depósito en Bitcoin. Ambas interfaces deben indicar cuándo se completa la transacción.

b. **Eficiencia (●):** Iniciar el pago no debe tomar más tiempo que un sistema de pago convencional. Una interfaz basada en web tendría la ventaja de que se puede cargar desde cualquier dispositivo con acceso a Internet. También necesita utilizar métodos de verificación rápidos para indicar si un pago ha sido propagado por la red Bitcoin. Aunque saber que una transacción ha sido propagada no es indicador de que la misma transacción ha sido verificada por la red, es un riesgo aceptable para un volumen bajo de transacciones.

c. **Tipo de cambio justo (●):** El sistema debe tener múltiples fuentes disponibles para la obtención de las tasas de intercambio para asegurar que se obtenga la tasa que más le convenga al cliente y para asegurar que no haya tiempos de inactividad del sistema (downtime).

d. **Disponibilidad (●):** La interfaz de pago debe estar abierta al público y debe poder cargarse en cualquier dispositivo.

2) Aplicabilidad

a. **Bajo costo de ejecución (●):** No existen costos de desarrollo ni de implementación para el sistema, incluso el hospedaje de la aplicación puede ser realizado de forma gratuita con soporte al volumen de transacciones esperado.

b. **Habilita la ramificación (●):** Dependiendo de la implementación, el soporte para sucursales adicionales solo implicaría ejecutar instancias adicionales de la aplicación en el servidor.

c. **Permite la conversión de divisas simultánea (●):** Debido a la volatilidad del precio de Bitcoin, es esencial poder realizar la conversión de

Bitcoin a dinero fiat (e.g. MXN[12] o USD[13]). Esta función deberá realizarse por medio de una institución financiera y deberá ser opcional para el negocio.

3) Privacidad

a. **Sin pérdida de información (●):** La interfaz de pagos no revela ninguna información sobre el sistema ni de la infraestructura interna de la empresa.

b. **Mantiene la privacidad del negocio (●):** Una nueva dirección es generada para cada solicitud de pago, por lo tanto, resulta imposible ver cuánto ha recibido la empresa en Bitcoin antes o después de cada transacción.

c. **Mantiene la privacidad del cliente (o):** Esta sería la responsabilidad del cliente y de la billetera Bitcoin que se esté utilizando y estaría fuera del alcance del sistema PoS.

d. **Lista de pagos confidenciales (●):** Una interfaz de administración y generación de reportes se encuentran disponibles al propietario de la empresa o al personal designado.

4) Seguridad

a. **Sin confianza a terceros (●):** No debería haber intercambio de información sensible entre los terceros en el sistema y debería poder funcionar como un sistema independiente. Cabe notar que, si bien se hace referencia a un tercero para las tasas de intercambio, los valores recibidos son tratados como una aserción que debe ser validada.

b. **Cifrado de datos (●):** Todas las claves privadas deben ser encriptadas y almacenadas en el servidor.

c. **Sin dependencia de software (●):** No debería existir ninguna dependencia de software en las pantallas de pago del negocio. Todas las dependencias de software en el lado del servidor deben incluirse en el paquete como software de código abierto.

B. *Librerías de código abierto y aplicaciones de software*

Después de la fase de ingeniería de requerimientos, se buscaron los componentes que formaran parte de la base del código. En base a la comparación de las pasarelas de pago disponibles que pueden adaptarse como punto de venta, Pyxpub parece cubrir la mayor parte de los requisitos para una implementación de un punto de venta y

[12] Peso mexicano
[13] dólar estadounidense

da la oportunidad de extender su funcionalidad y de diseñar la infraestructura en base a los requerimientos de cualquier negocio.

Pyxpub es un software 100 % gratuito y de código abierto (open source[14]) que ofrece las siguientes características, que lo hacen perfecto para su uso como un sistema de punto de venta.

- **Privacidad:** Permite recibir pagos de manera privada, generando direcciones y números de orden únicos con cada pago que protegen la privacidad del negocio y del cliente.
- **Seguridad:** El sistema funciona dentro de su propio ecosistema. No se transmiten datos entre el servidor y terminal que puedan comprometer la seguridad de los pagos. Pyxpub aplica las mejores prácticas de Bitcoin para asegurar el sistema.
- **Rapidez:** El sistema valida las transacciones de manera instantánea sin la necesidad de esperar a las confirmaciones en la red. La tecnología pero asegurar pagos instantáneos y verificables.
- **Fácil escalabilidad e implementación:** Permite una implementación directa, de manera local o en algún servidor web. El software puede ejecutarse en una computadora personal o cualquier hardware simple y barato como un Raspberry Pi.
- **Moderno:** Basado en tecnologías web y de pago modernas que hacen que la experiencia de pago lo más fluida posible.
- **$€¥ Múltiples divisas:** Compatible con más de 30 monedas diferentes, junto con una amplia variedad de fuentes de tipo de cambio.

Pyxpub se compone por dos partes principales, una API (back-end) desarrollada en Python[15] que permite exponer las características necesarias de una billetera de sólo recepción, y una interfaz web (front-end) desarrollada en ReactJS[16] que permite a un usuario interactuar con esta API. A continuación es enlistan las librerías principales utilizadas por estos componentes:

- **Django**[17]: Framework web de alto nivel que permite el desarrollo rápido de sitios web seguros y mantenibles. Django se encarga de gran parte de las complicaciones del desarrollo web.

[14] Tipo de software que se distribuye mediante una licencia que le permite al usuario final, si tiene los conocimientos necesarios, utilizar el código fuente del programa para estudiarlo, modificarlo y realizar mejoras en el mismo, pudiendo incluso hasta redistribuirlo.
[15] https://www.python.org/
[16] https://reactjs.org/
[17] https://www.djangoproject.com/

- **pycoin**[18]: Biblioteca de utilidades Bitcoin y alt-coins[19] basadas en Python.
- **qrcode**[20]: Generación de códigos QR
- **cashaddress**[21]: Herramienta que permite la conversión entre distintos formatos de direcciones.

Un desglose de las funciones que Pyxpub nos proporciona son las siguientes:

- **Generación de direcciones de Bitcoin:** Pyxpub utiliza pycoin para la generación de direcciones. Todas las direcciones generadas se derivan de una clave XPUB[22] predefinida. Se evita la reutilización de direcciones al realizar un seguimiento de las direcciones previamente utilizadas.
- **Interfaz de entrada:** Tiene herramientas y métodos básicos que permite la generación de solicitudes de pago por medio de interfaces de entrada.
- **Confirmación de pagos:** Se utilizan APIs de herramientas web que permiten validar el estado de las transacciones. Estas fuentes son configurables.

Sin embargo, carece de algunas otras características que deben implementarse:

- **Base de datos:** Pyxpub tiene una implementación muy básica de base de datos. Actualmente utiliza un archivo local en el directorio del proyecto. Es necesario implementar una integración a una base de datos remota si fuera necesario.
- **Conversión entre fiat y cripto:** Es necesario implementar una forma de convertir los pagos recibidos a dinero fiat de manera instantánea.
- **Tasa de intercambio:** Hay fuentes predefinidas de tasas de intercambio para realizar las conversiones en la aplicación. Estas tasas son obtenidas de servicios web que ofrecen múltiples divisas que permiten convertir montos entre dinero fiat y criptomoneda, sin embargo, Pyxpub contiene varias fuentes que necesitan actualizarse (por cambios de API) y también es necesario agregar fuentes nuevas que tengan mejor soporte para MXN.
- **Página de reportes:** Es necesario agregar una página de reportes que permita ver y exportar información de las ventas (entre otra información).

[18] https://github.com/richardkiss/pycoin
[19] Criptomonedas alternativas a Bitcoin
[20] https://github.com/lincolnloop/python-qrcode
[21] https://github.com/oskyk/cashaddress
[22] Una clave pública extendida, también conocida como XPUB, es parte del estándar BIP32 de Bitcoin que puede considerarse como una billetera de 'solo lectura'. XPUB permite una vista completa del historial de todas las transacciones, direcciones y balances en una billetera específica, pero no permite gastos de ningún tipo (a diferencia de la llave privada). Esta clave también es de donde se derivan todas las direcciones Bitcoin de la billetera.

C. *Prototipado*

Con el conocimiento completo de los requerimientos se comenzó a trabajar en el prototipado de la aplicación y se optó por la siguiente arquitectura:

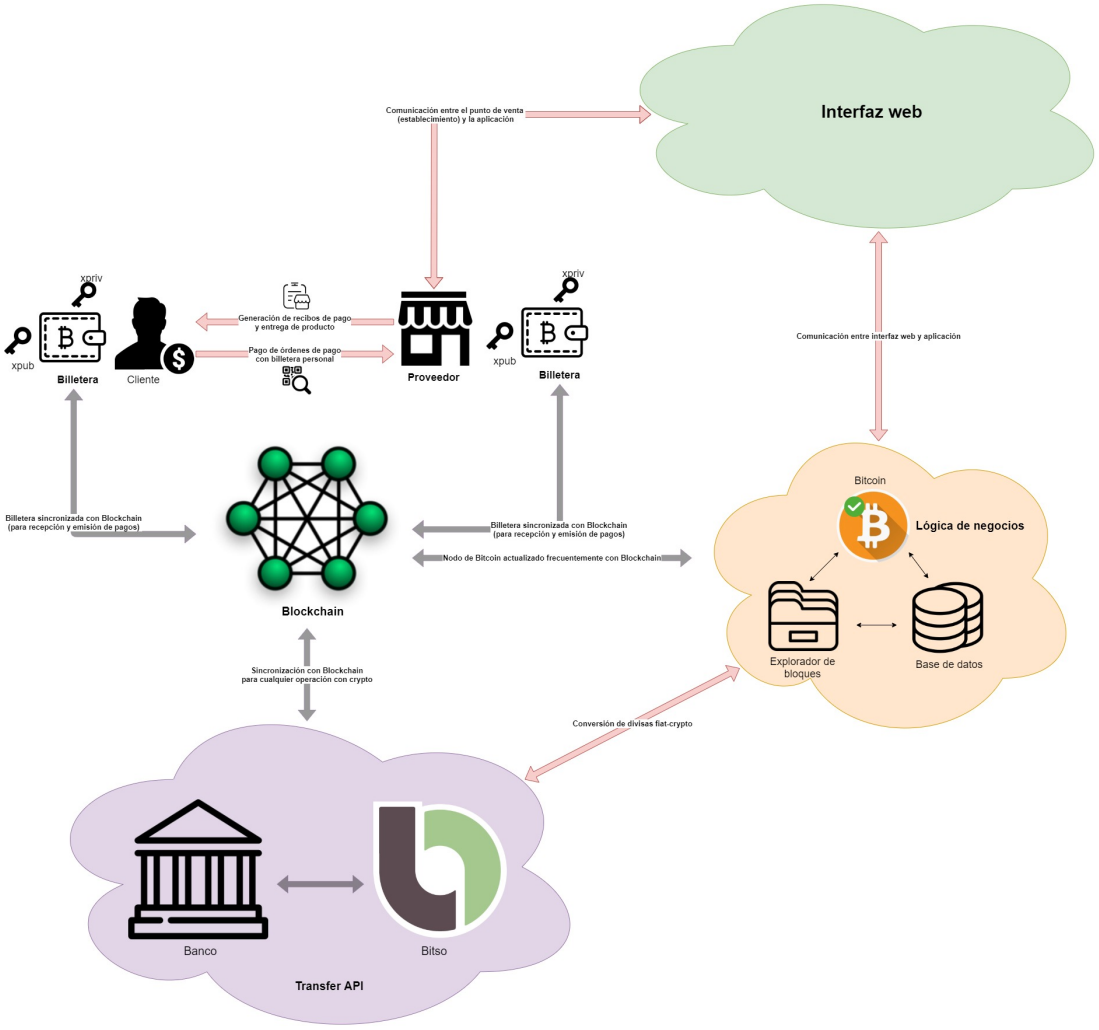


FIGURA 3.2: Arquitectura del nuevo sistema de pagos con Blockchain

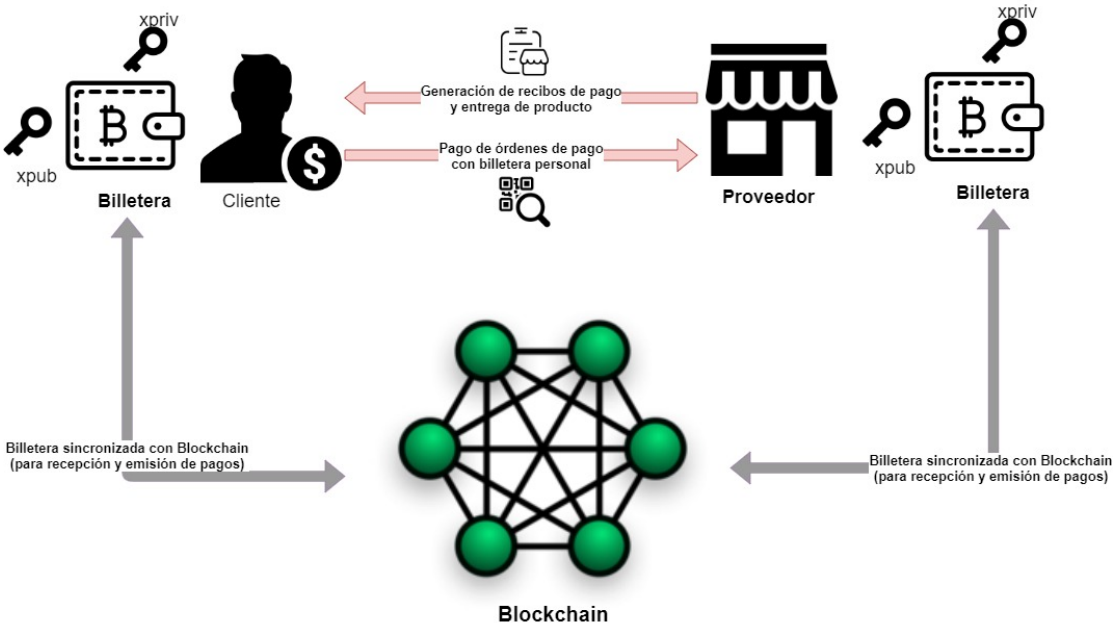


FIGURA 3.3: Interacción cliente-negocio

La interacción comienza con un cliente dentro de un establecimiento con la intención de pagar por un producto o servicio ofrecido, suponiendo que el cliente tiene conocimiento básico del funcionamiento de Blockchain, y Bitcoin para nuestros propósitos, y que ya cuenta con una billetera digital con los montos necesarios para cubrir el servicio. La forma de comprar o configurar una billetera digital Bitcoin se encuentra fuera del enfoque de este trabajo.

- Al momento del pago, utilizando la interfaz web, el proveedor puede generar solicitudes de pago (Figura 3.8) con el monto necesario.
- Junto con la solicitud de pago se genera una dirección Bitcoin, que es única para esa solicitud (por propósitos de validación), y un código QR[23] que contiene la información del pago, y el cual el cliente escanea con su dispositivo móvil (Figura 3.9). Todas las billeteras digitales tienen algún tipo de soporte para leer estos códigos. Al momento de escanear el código, el cliente puede verificar la dirección y monto requerido en su dispositivo antes de confirmar el pago.
- Mientras tanto, la aplicación revisa el estado de esa dirección con un explorador de bloques[24] para verificar que se haya mandado el pago. Al momento de validar la dirección con el monto requerido, se muestra una pantalla de confirmación al usuario (Figura 3.10).

[23]Los códigos QR (Quick Response) son códigos de barras, capaces de almacenar determinado tipo de información, como una URL, SMS, email, texto, etc.

[24]Un explorador de bloques es una aplicación web, generalmente disponible en línea a través de un navegador web, que proporciona varios datos de una red blockchain específica. Permite a los usuarios extraer datos importantes sobre transacciones criptográficas, como direcciones y tarifas.

FIGURA 3.4: Servicio de intercambio Bitso

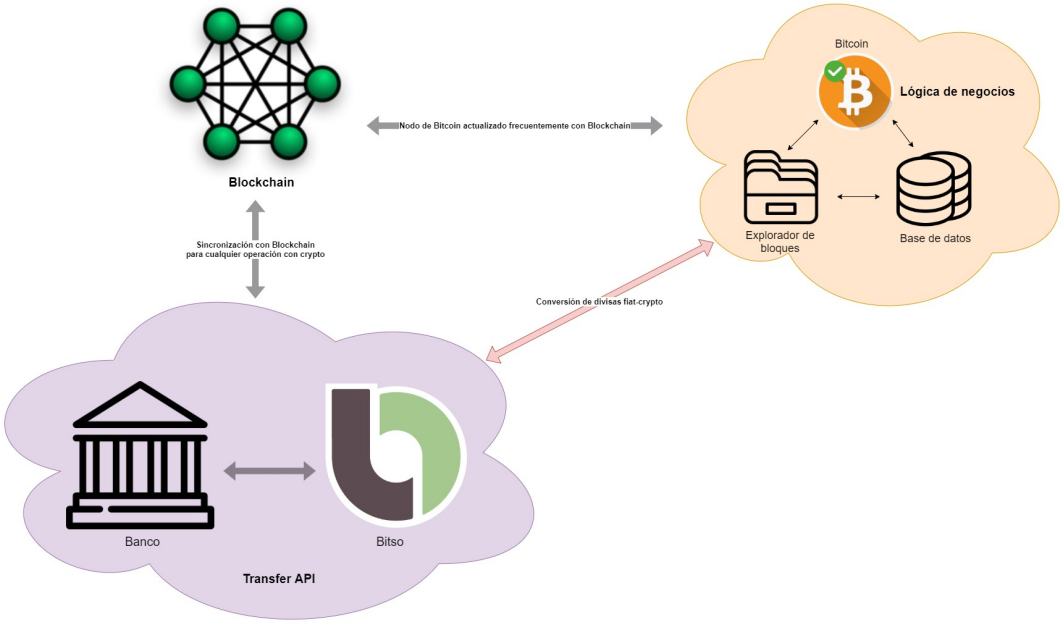


FIGURA 3.5: Integración del sistema con Transfer API por medio de Bitso

Para permitir la conversión de Bitcoin a moneda nacional se hace uso del servicio de intercambio Bitso[25] y de su API denominada Transfer API. Es necesario registrar y configurar una cuenta en el servicio para el acceso de esta funcionalidad (Figura 3.6). Es por el uso de esta API que se generan las direcciones Bitcoin para las solicitudes de pago y por la cual se realiza la conversión de Bitcoin a dinero fíat (moneda nacional). El proceso es el siguiente:

- Es posible configurar las salidas de pago dentro de la aplicación para recibir ya sea Bitcoin, con una dirección pública ya previamente definida, o moneda nacional (MXN), con una cuenta CLABE para la recepción de pesos mexicanos después de la conversión (Figura 3.7).

[25] https://bitso.com/

- Al momento de generar una solicitud de pago en la aplicación, se hace una cotización del monto actual de moneda nacional a Bitcoin. Esta cotización contiene la tasa de intercambio necesaria para recibir ese monto en pesos mexicanos al momento de la conversión. Este monto es válido por 30 segundos, por lo que es necesario refrescar la tasa de manera automática para asegurar que el monto recibido sea el correcto. Asimismo, en esta misma cotización se incluye una dirección Bitcoin a donde es necesario enviar el monto especificado.
- Con esta dirección Bitcoin recibida, se genera una historial de pago para futuras referencias, y se genera el código QR al usuario para recibir su pago (Figura 3.9).
- Al momento de recibir el pago y ser verificado, Bitso realiza la conversión de manera automática y envía los fondos a la cuenta de banco previamente especificada (Figura 3.12).

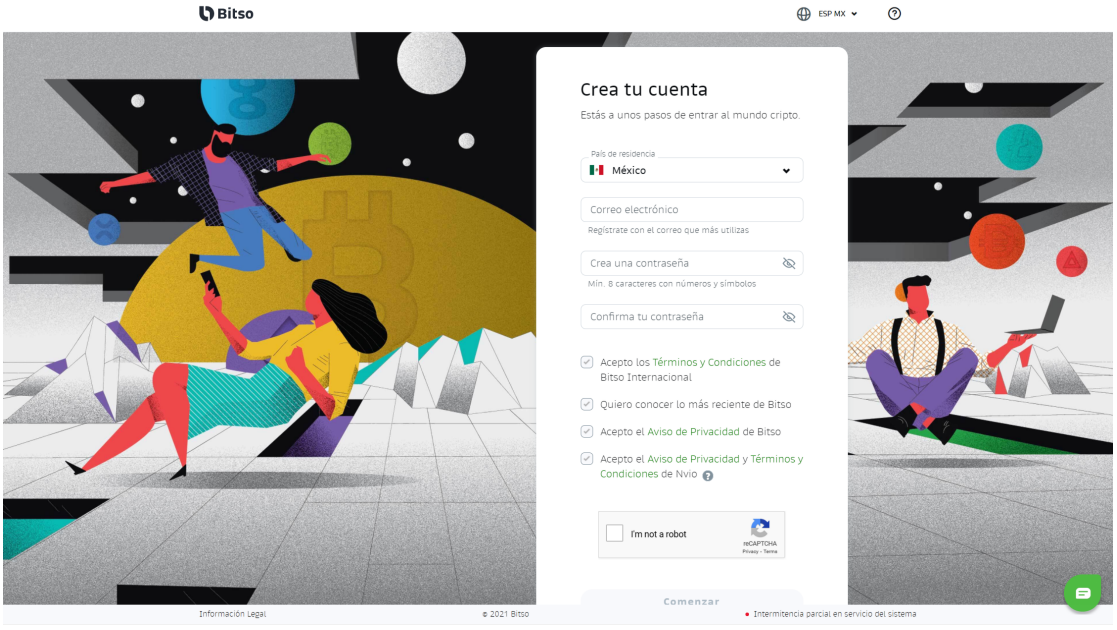


FIGURA 3.6: Registro en el servicio de intercambio de Bitso

FIGURA 3.7: Configuración de las salidas de pago

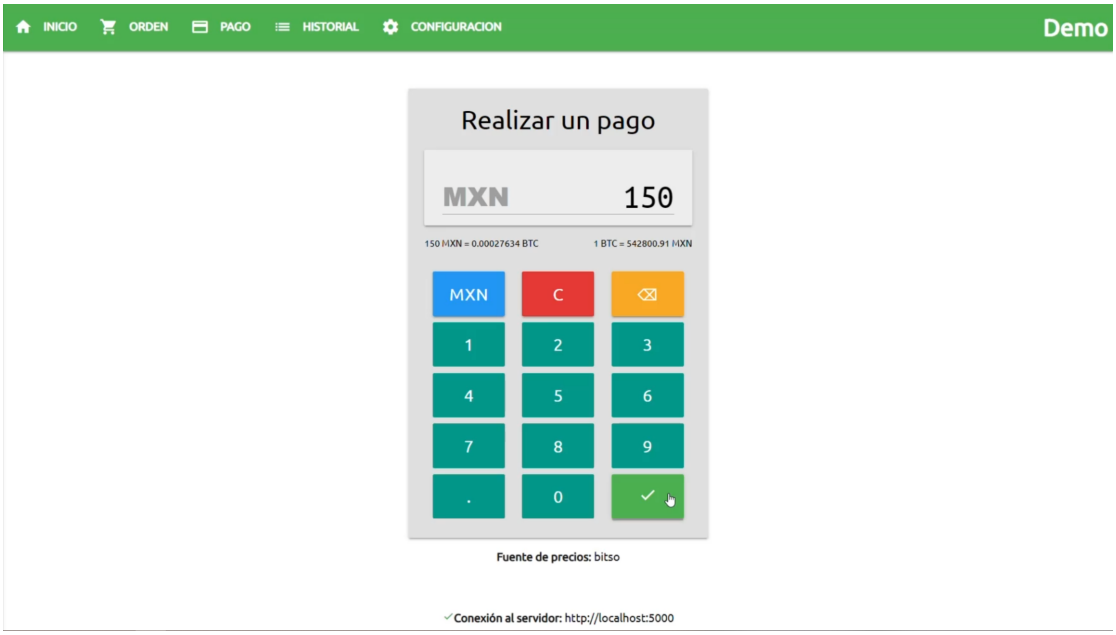


FIGURA 3.8: Terminal para la generación de solicitudes de pago

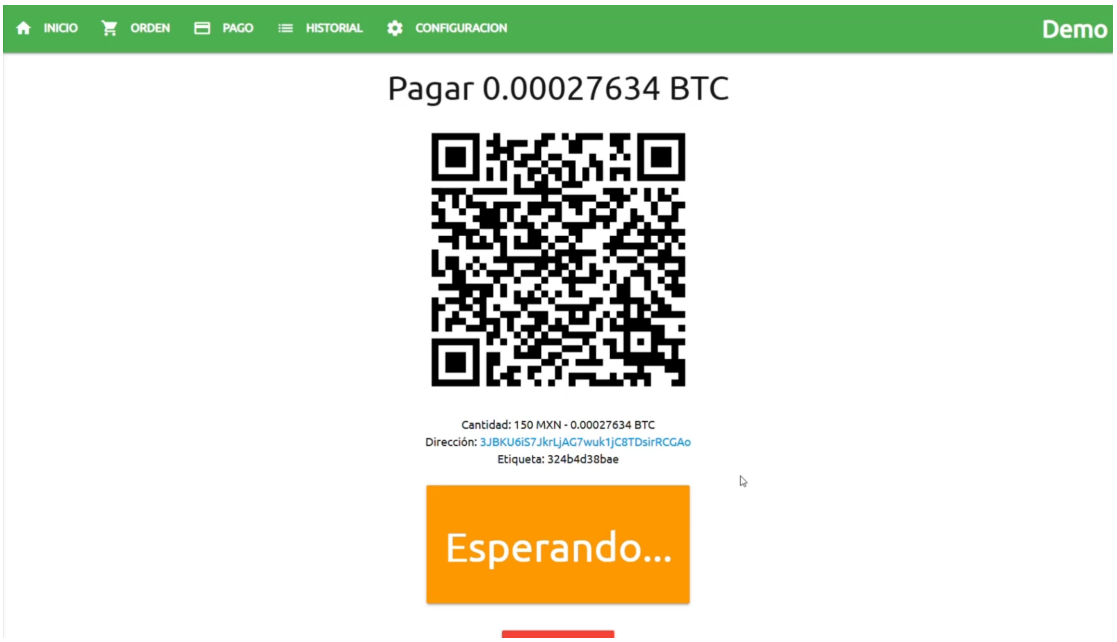


FIGURA 3.9: Solicitud de pago generada con el monto seleccionado

FIGURA 3.10: Pantalla de confirmación para un pago recibido

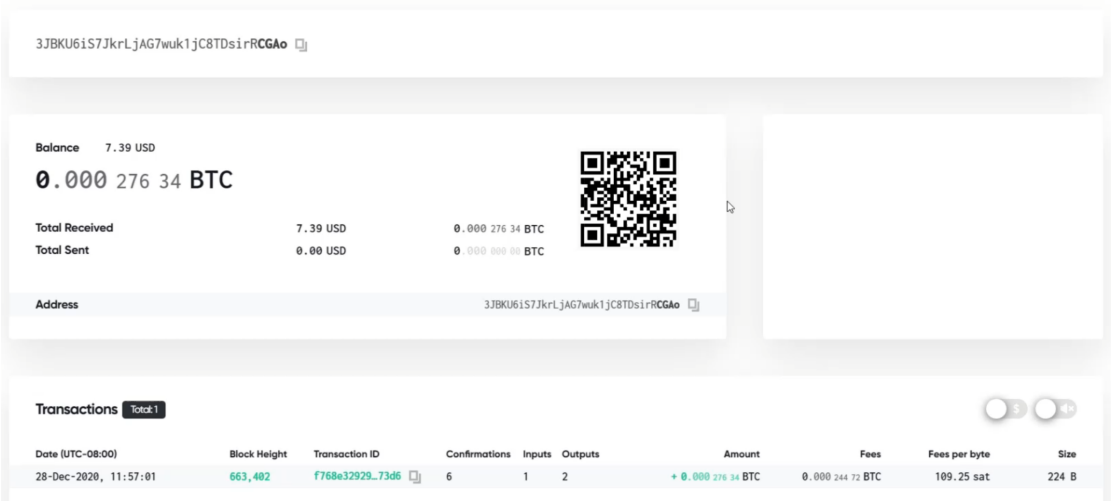


FIGURA 3.11: Ejemplo de un explorador de bloques conteniendo la información del pago

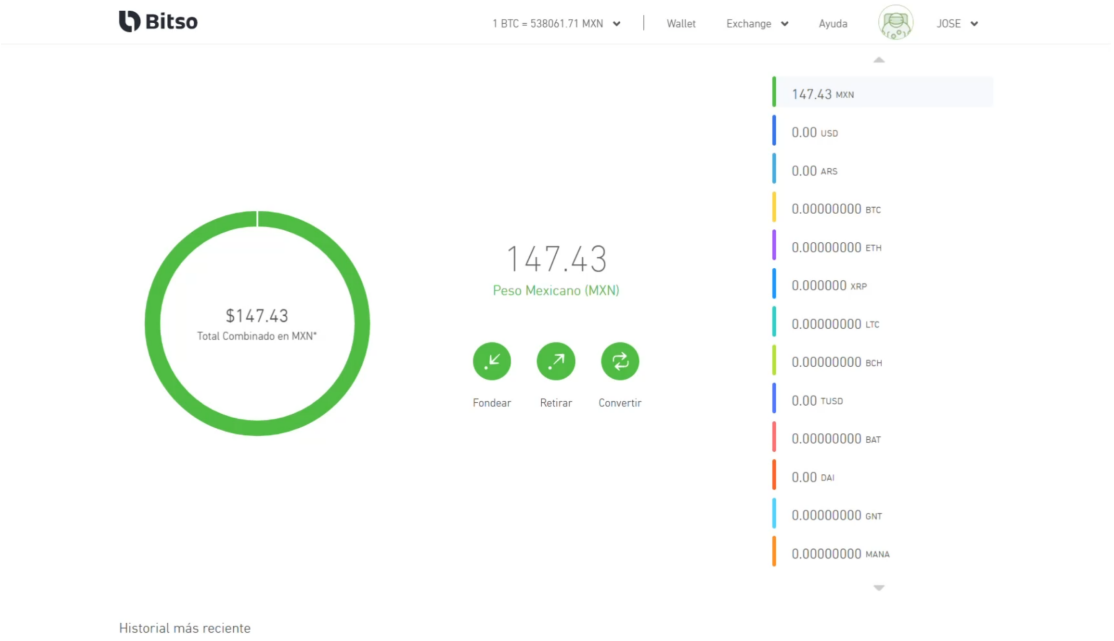


FIGURA 3.12: Conversión de un pago a moneda nacional

4 Conclusiones

Considerando los requerimientos del marco de evaluación definidos, se realizó un nueva comparación de las soluciones actuales para recepción de pagos con el sistema desarrollado:

a. **Usabilidad**

   El sistema conforma un servidor (para la lógica de negocios, como la conversión de divisas, tasas de intercambio, etc.) y una interfaz web, la cual permite la configuración completa para la recepción de pagos. Se presenta con un diseño amigable y sencillo (Facilidad de uso: •, Eficiencia: •). Las tasas de intercambio al momento de un pago se obtienen de manera real, con fuentes confiables (Tipo de cambio justo: •). La aplicación se ejecuta de manera local en cualquier dispositivo, con el único requerimiento siendo la conectividad a internet para realizar la conversión y validación de pagos (Disponibilidad: •).

b. **Aplicabilidad**

   Por el hecho de que la aplicación se configura de manera local, en el establecimiento, no incluye costos adicionales para su implementación (Bajo costo de ejecución: •). La implementación también se puede configurar en cada establecimiento de manera individual, y sin ningún límite (Habilita la ramificación: •). Es posible configurar la salida de pagos de forma digital (Bitcoin) o en moneda nacional (MXN). La conversión a moneda nacional se realiza en tiempo real, al momento de recibir un pago, por lo que se asegura recibir las cantidades correctas, basadas en la tasa de intercambio al momento (Permite la conversión de divisas simultánea: •).

c. **Privacidad**

   Para cada solicitud de pago, una nueva dirección Bitcoin es generada. Esto para asegurar el correcto seguimiento de cada pago, y para asegurar la privacidad de ambas partes (Mantiene la privacidad del negocio: •, Mantiene la privacidad del cliente: •). La única información requerida para el funcionamiento del sistema es una llave pública (obtenida de cualquier billetera Bitcoin disponible) para usar

como base en la generación de direcciones para la recepción de pagos. Se genera una nueva dirección Bitcoin para cada solicitud de pago para mantener la privacidad de ambas partes . Todas las solicitudes de pago son almacenadas en una base de datos para su acceso posterior (Lista de pagos confidenciales: •).

d. **Seguridad**

El sistema se ejecuta de manera independiente a un servidor. Todas las operaciones como el cálculo de tasas de intercambio o conversión de divisas se realizan dentro de la aplicación (Sin dependencia de software: •, Sin confianza a terceros: •). Ninguna información personal del negocio sale de la aplicación, ya que es ejecutada de manera local, dentro del mismo establecimiento. (Cifrado de datos: •).

Categoría	Facilidad de uso	Eficiencia	Tipo de cambio justo	Disponibilidad	Bajo costo de ejecución	Habilita la ramificación	Conversión de divisas simultánea	Mantiene la privacidad del negocio	Mantiene la privacidad del cliente	Lista de pagos confidenciales	Sin confianza a terceros	Cifrado de datos	Sin dependencia de software
Dirección Bitcoin en mostrador				•	•	◦			◦		•		•
Terminales de hardware	◦	•	◦	•				•	•	•		•	
Servicios comerciales en línea	•	•	◦	◦	•	•		•	•	◦		◦	•
Mycelium Gear	◦	•	◦	◦	◦	•		•	•	◦	◦	◦	◦
Pyxpub	•	•	•	•	•	•		•	•	•	•	•	•
Bitcoin PoS	•	•	•	•	•	•	•	•	•	•	•	•	•

FIGURA 4.1: Comparación de pasarelas de pago con el sistema desarrollado

Por lo presentado anteriormente, se observa que el sistema propuesto cubre los requerimientos definidos en el marco de evaluación, teniendo las ventajas combinadas que provee un sistema de punto de venta (PoS) y la tecnología Blockchain. Este trabajo demuestra la viabilidad de un sistema de punto de venta que integra esta tecnología, pero que considera sus limitaciones y desventajas. Asimismo, le brinda atención a este tipo de tecnologías y promueve la adopción en sectores que aún no lo consideran.

Bibliografía

[1] Alford, M. (2002). *Software Requirements Engineering Methodology*. American Cancer Society.

[2] Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., and Capkun, S. (2013). Evaluating user privacy in bitcoin. In *International Conference on Financial Cryptography and Data Security*, pages 34–51. Springer.

[3] Beck, R., Czepluch, J. S., Lollike, N., and Malone, S. (2016). Blockchain-the gateway to trust-free cryptographic transactions. In *ECIS*, page ResearchPaper153.

[4] Bevan, N. (1995). Usability is quality of use. In *Advances in Human Factors/Ergonomics*, volume 20, pages 349–354. Elsevier.

[5] Bonneau, J., Herley, C., Oorschot, P. C. v., and Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. Technical report, University of Cambridge, Computer Laboratory.

[6] Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J., and Felten, E. (2014). Mixcoin: Anonymity for bitcoin with accountable mixes. In Safavi-Naini, R. and Christin, N., editors, *Financial Cryptography and Data Security - 18th International Conference, FC 2014, Revised Selected Papers*, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pages 486–504. Springer Verlag. 18th International Conference on Financial Cryptography and Data Security, FC 2014 ; Conference date: 03-03-2014 Through 07-03-2014.

[7] Burchert, C., Decker, C., and Wattenhofer, R. (2018). Scalable funding of bitcoin micropayment channel networks. *Royal Society Open Science*, 5(8).

[8] Chaum, D. (1983). Blind signatures for untraceable payments. In *Advances in cryptology*, pages 199–203. Springer.

[9] Chen, P., Jiang, B., and Wang, C. (2017). Blockchain-based payment collection supervision system using pervasive bitcoin digital wallet. In *2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 139–146.

[10] Decker, C. and Wattenhofer, R. (2015). A fast and scalable payment network with bitcoin duplex micropayment channels. In Pelc, A. and Schwarzmann, A. A., editors, *Stabilization, Safety, and Security of Distributed Systems*, pages 3–18, Cham. Springer International Publishing.

[11] Dorfman, M. (1990). Requirements engineering.

[12] Engelmann, F., Kopp, H., Kargl, F., Glaser, F., and Weinhardt, C. (2017). Towards an economic analysis of routing in payment channel networks. In *Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers*, SERIAL '17, pages 2:1–2:6, New York, NY, USA. ACM.

[13] Ernstberger, P. (2009). Linden dollar and virtual monetary policy.

[14] Fauzi, M. R. R., Nasution, S. M., and Paryasto, M. W. (2017). Implementation and analysis of the use of the blockchain transactions on the workings of the bitcoin. *IOP Conference Series: Materials Science and Engineering*, 260(1):012003.

[15] Gobel, J. and Krzesinski, A. (2017). Increased block size and bitcoin blockchain dynamics. In *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, pages 1–6. IEEE.

[16] Green, M. and Miers, I. (2017). Bolt: Anonymous payment channels for decentralized currencies. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 473–489. ACM.

[17] Herrera-Joancomartí, J. and Pérez-Solà, C. (2016). Privacy in bitcoin transactions: New challenges from blockchain scalability solutions. In Torra, V., Narukawa, Y., Navarro-Arribas, G., and Yañez, C., editors, *Modeling Decisions for Artificial Intelligence*, pages 26–44, Cham. Springer International Publishing.

[18] Hu, Y., Manzoor, A., Ekparinya, P., Liyanage, M., Thilakarathna, K., Jourjon, G., Seneviratne, A., and Ylianttila, M. E. (2018). A delay-tolerant payment scheme based on the ethereum blockchain. *arXiv preprint arXiv:1801.10295*.

[19] Im, S. (2012). Web integrated point-of-sale system. US Patent App. 13/112,718.

[20] Kaplanov, N. (2012). Nerdy money: Bitcoin, the private digital currency, and the case against its regulation. *Loy. Consumer L. Rev.*, 25:111.

[21] Kaushik, A., Choudhary, A., Ektare, C., Thomas, D., and Akram, S. (2017). Blockchain — literature survey. In *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT)*, pages 2145–2148.

[22] Khalil, R. and Gervais, A. (2017). Revive: Rebalancing off-blockchain payment networks. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 439–453. ACM.

[23] KOTESKA, B., KARAFILOSKI, E., and MISHEV, A. (2017). Blockchain implementation quality challenges: A literature. In *SQAMIA 2017: 6th Workshop of Software Quality, Analysis, Monitoring, Improvement, and Applications*, pages 11–13.

[24] Kwon, J. (2014). Tendermint: Consensus without mining. *Draft v. 0.6, fall.*

[25] Laxmaiah, M. and Neha, T. (2019). A novel approach for digital online payment system. In Kumar, A. and Mozar, S., editors, *ICCCE 2018*, pages 703–712, Singapore. Springer Singapore.

[26] Lind, J., Eyal, I., Kelbert, F., Naor, O., Pietzuch, P., and Sirer, E. G. (2017). Teechain: Scalable blockchain payments using trusted execution environments. *arXiv preprint arXiv:1707.05454*.

[27] Luther, W. J. (2016). Bitcoin and the future of digital payments. *The Independent Review*, 20(3):397–404.

[28] McCorry, P., Möser, M., Shahandasti, S. F., and Hao, F. (2016). Towards bitcoin payment networks. In Liu, J. K. and Steinfeld, R., editors, *Information Security and Privacy*, pages 57–76, Cham. Springer International Publishing.

[29] Miers, I., Garman, C., Green, M., and Rubin, A. D. (2013). Zerocoin: Anonymous distributed e-cash from bitcoin. *2013 IEEE Symposium on Security and Privacy*, pages 397–411.

[30] Min, X., Li, Q., Liu, L., and Cui, L. (2016). A permissioned blockchain framework for supporting instant transaction and dynamic block size. In *Trustcom/BigDataSE/ISPA, 2016 IEEE*, pages 90–96. IEEE.

[31] Molka-Danielsen, J. and Deutschmann, M. (2009). *Learning and teaching in the virtual world of Second Life*. tapir academic Press.

[32] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[33] Network, F. C. E. (2013). Application of fincen's regulations to persons administering, exchanging, or using virtual currencies. *United States Department of the Treasury, March*, 18.

[34] Niranjanamurthy, M., Nithya, B., and Jagannatha, S. (2018). Analysis of blockchain technology: pros, cons and swot. *Cluster Computing*, pages 1–15.

[35] Nofer, M., Gomber, P., Hinz, O., and Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, 59(3):183–187.

[36] Research and Markets (2018). Cloud pos market by component, organization size, application area (retail and consumer goods, travel and hospitality, transportation and logistics, media and entertainment, and healthcare), and region - global forecast to 2023. *URl: https://www.researchandmarkets.com/research/6j7t8g/3_7billion*.

[37] Saito, K. and Yamada, H. (2016). What's so different about blockchain?—blockchain is a probabilistic state machine. In *Distributed Computing Systems Workshops (ICDCSW), 2016 IEEE 36th International Conference on*, pages 168–175. IEEE.

[38] Samuelson, P. A. (1968). What classical and neoclassical monetary theory really was. *The Canadian Journal of Economics/Revue canadienne d'Economique*, 1(1):1–15.

[39] Sidhu, J. (2017). Syscoin: A peer-to-peer electronic cash system with blockchain-based services for e-business. In *Computer Communication and Networks (ICCCN), 2017 26th International Conference on*, pages 1–6. IEEE.

[40] Singh, S. and Singh, N. (2016). Blockchain: Future of financial and cyber security. In *Contemporary Computing and Informatics (IC3I), 2016 2nd International Conference on*, pages 463–467. IEEE.

[41] Stephen, R. and Alex, A. (2018). A review on blockchain security. *IOP Conference Series: Materials Science and Engineering*, 396(1):012030.

[42] Sun, H., Mao, H., Bai, X., Chen, Z., Hu, K., and Yu, W. (2017). Multi-blockchain model for central bank digital currency. In *Parallel and Distributed Computing, Applications and Technologies (PDCAT), 2017 18th International Conference on*, pages 360–367. IEEE.

[43] Sutcliffe, A. (1998). Scenario-based requirements analysis. *Requirements engineering*, 3(1):48–65.

[44] Sutcliffe, A. G. (2003). Scenario-based requirements engineering. *Proceedings. 11th IEEE International Requirements Engineering Conference, 2003.*, pages 320–329.

[45] Tama, B. A., Kweka, B. J., Park, Y., and Rhee, K. (2017). A critical review of blockchain and its current applications. In *2017 International Conference on Electrical Engineering and Computer Science (ICECOS)*, pages 109–113.

[46] Vranken, H. (2017). Sustainability of bitcoin and blockchains. *Current Opinion in Environmental Sustainability*, 28:1–9.

[47] Wang, Y. and Kogan, A. (2018). Designing confidentiality-preserving blockchain-based transaction processing systems. *International Journal of Accounting Information Systems*, 30:1–18.

[48] Wuille, P. (2012). Hierarchical deterministic wallets. https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki.

[49] Wuille, P. (2016). Hierarchical deterministic wallets. 2012. *URl: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki*.

[50] Xia, Q., Sifah, E. B., Huang, K., Chen, R., Du, X., and Gao, J. (2018). Secure payment routing protocol for economic systems based on blockchain. In *2018 International Conference on Computing, Networking and Communications (ICNC)*, pages 177–181. IEEE.

[51] Yamada, Y., Nakajima, T., and Sakamoto, M. (2016). Blockchain-li: A study on implementing activity-based micro-pricing using cryptocurrency technologies. In *Proceedings of the 14th International Conference on Advances in Mobile Computing and Multi Media*, pages 203–207. ACM.

[52] Zhang, Y., Deng, R., Liu, X., and Zheng, D. (2018). Outsourcing service fair payment based on blockchain and its applications in cloud computing. *IEEE Transactions on Services Computing*.

[53] Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *Big Data (BigData Congress), 2017 IEEE International Congress on*, pages 557–564. IEEE.

[54] Zhu, Q., Wang, T., and Jia, Y. (2007). Second life: A new platform for education. In *Information Technologies and Applications in Education, 2007. ISITAE'07. First IEEE International Symposium on*, pages 201–204. IEEE.

[55] Zhu, Y., Riad, K., Guo, R., Gan, G., and Feng, R. (2018). New instant confirmation mechanism based on interactive incontestable signature in consortium blockchain. *Frontiers of Computer Science*.