UNIVERSIDAD LA SALLE

FACULTAD DE CIENCIAS DE LA INGENIERÍA

CARRERA DE INGENIERÍA DE SISTEMAS

CARTERA MÓVIL DIGITAL DE DINERO VIRTUAL BITCOIN PARA MICROEMPRESAS BOLIVIANAS

Caso: "Cerámicas Jiwasa"

Por

Gabriela Melendrez Alaro

Tutor: Dr. Ing. René Reynaga

Proyecto de grado presentada para la obtención del Grado de Licenciatura en Ingeniería de Sistemas

La Paz – Bolivia

2014

AGRADECIMIENTOS

Ante todo a Dios, a mi familia por su paciencia y cariño. A mi tutor Dr. Ing. René Reynaga por su contribución e Ing. Walter Carvajal por su permanente apoyo y al revisor Ing. Carlos Arteaga por los concejos.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Se ha desarrollado un sistema de moneda digital dentro del área de los microempresarios; la aplicación móvil de moneda digital Bitcoin permitirá saber la evolución de esta moneda, como el tipo de cambio y conocer las diferentes transacciones de monedas centralizadas por el Bitcoin (BTC). La cartera móvil para acciones comerciales en microempresas Bolivianas tal es el caso de Cerámicas Jiwasa, tiene como propósito la expansión de la moneda digital Bitcoin (BTC) en la economía global, teniendo como objetivo general desarrollar un prototipo de cartera móvil que permita estar informado de la economía del Bitcoin. Por lo que, este proyecto da a conocer una alternativa más dentro de las divisas, el dinero digital "Bitcoin" que no trabaja con terceros de confianza, tiene valor único a nivel mundial, acceso sin prerrequisitos; por las diferentes ventajas que esta presenta nos centramos a las transacciones dentro de las microempresas que no tienen la posibilidad de trabajar con bancos o simplemente plantear la reducción de costos a las microempresas que trabajan con bancos, se propone una solución al problema doble gasto mediante una red peer to peer.

Al realizar el análisis de los problemas que presenta el comercio electrónico, Satoshi Nakamoto (Nakamoto, 2009), referente a la creación del dinero digital Bitcoin, hace referencia a este tema de la dependencia casi exclusivamente de las instituciones financieras en calidad de terceros de confianza para el procesamiento de pagos electrónicos; el costo de la

mediación aumenta los costos de transacción, además los terceros de confianza limitan el tamaño mínimo de transacción práctica y corta la posibilidad de que pequeñas empresas realicen transacciones imprevistas. Así mismo, para la interacción con otras divisas un microempresario debe cumplir prerrequisitos para optar por una cuenta bancaria además que al momento de realizar transacciones el banco cobra ciertas comisiones.

I. MARCO REFERENCIAL

1.1. Introducción

La cartera móvil digital para acciones comerciales en microempresas bolivianas tal es el caso de Cerámicas Jiwasa, tiene como propósito la expansión de la moneda digital Bitcoin (BTC) en la economía global, teniendo como objetivo general desarrollar un prototipo de cartera móvil digital que permita estar informado de la economía del Bitcoin, el proyecto no solo se queda en la instalación de la billetera digital si no propone su funcionamiento como banca digital personalizada una aplicación web 2.0 donde nos indicara los diferentes datos de la evolución del dinero digital Bitcoin, todos los datos bajados desde la nube, además permite saber la evolución de esta moneda, como el tipo de cambio y conocer las diferentes transacciones en BTC. Por lo que comprenderemos las ventajas que origina el simple hecho de trabajar sin intermediarios, *ser nuestro propio banco,* dando así una nueva alternativa a las microempresas, en particular a Cerámica Jiwasa.

El aporte básico a la economía Bitcoin es la cartera móvil digital realizada exclusivamente para Bitcoin.

Además conoceremos de manera profunda cada una de las herramientas y modelos que serán utilizadas en el desarrollo del presente proyecto, conociendo más acerca de las características del dinero Bitcoin así como el funcionamiento, origen y las diferentes utilidades que ya podemos encontrar en el mercado global.

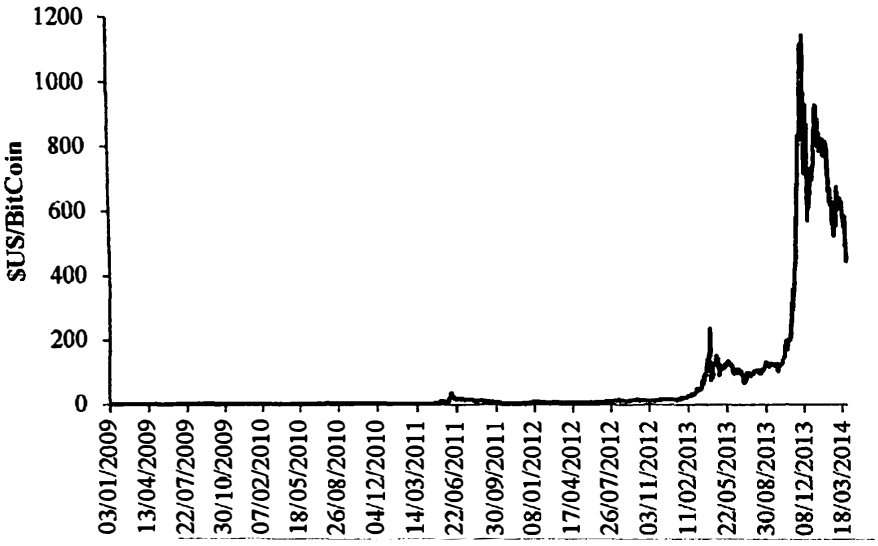
1.2. Antecedentes

Gran parte de la población que trabaja con los bancos sabe que los servicios que el cliente use serán realizados a cambio del pago de una comisión que en caso de la microempresas puede ser significante en la estructura de precios, quitándole competitividad a nivel internacional. Se decide, tener como área de estudio a los microempresarios, ya que en Bolivia las grandes cuentas en los bancos son de empresas privadas grandes y los microempresarios no tienen esa facilidad de adquirir una cuenta en el banco ya que implica cumplir acuerdos limitados y si tienen una cuenta en el banco limita el tamaño mínimo de transacciones y corta la posibilidad de realizar pequeñas transacciones, si bien este problema tal vez la solución más sencilla seria trabajar con dinero físico, ya que no se manejarían cifras grandes de dinero pero no existe ningún mecanismo para hacer los pagos a lo largo de un canal de comunicación sin un tercero de confianza. Como una solución a este problema emergen algunas monedas alternativas, lo que es "el dinero digital" como por ejemplo la moneda de facebook; facebook credits, Amazoninc de Amazon y los Bitcoin la primera moneda digital más importante, pero también encontramos monedas digitales tales son los casos de LiteCoin, PeerCoin, AuroraCoin, DogeCoin, Namecoin, Tonal Bitcoin, IxCoin, Devcoin, Freicoin, 10coin, Liquidcoin, Quark, Primecoin, Feathercoin y Ripple; cada una de estas monedas presentan ciertas ventajas, pero a la que se analizara y la que se implementara en el prototipo será el Bitcoin.

Un referente como crecida en la expansión del Bitcoin es el precio del Bitcoin, ya que se lo viene estudiando desde 2012 y a la fecha su precio tomó más peso, como se puede apreciar en la Figura 1 que muestra el valor grafico del Bitcoin como valor estable durante su creación hasta el valor obtenido para

inicio del 2013, donde el precio del Bitcoin empieza a variar a partir del 2013 presentando así la crecida de precio Bitcoin.

Figura 1: Crecimiento del precio del Bitcoin 2009 - 2014



Fuente: The Economics of Bitcoin Price Formation
http://www.quandl.com/markets/BitCoin

El Bitcoin es otra alternativa más en divisa valorada a nivel mundial, el "Bitcoin" es una moneda digital creada a principios de 2009 por el japonés Satoshi Nakamoto (Nakamoto, 2009) que tiene la peculiaridad de no estar atada a una administración central por parte de las autoridades, y que empezó a hacerse popular hace poco tiempo.

"Bitcoin es una moneda del futuro es 100% digital, segura, y a diferencia del dinero tradicional no está controlada por los bancos". (Bilitelia, 2012)

A menos que su uso sea limitado por entidades de dominio gubernamental.

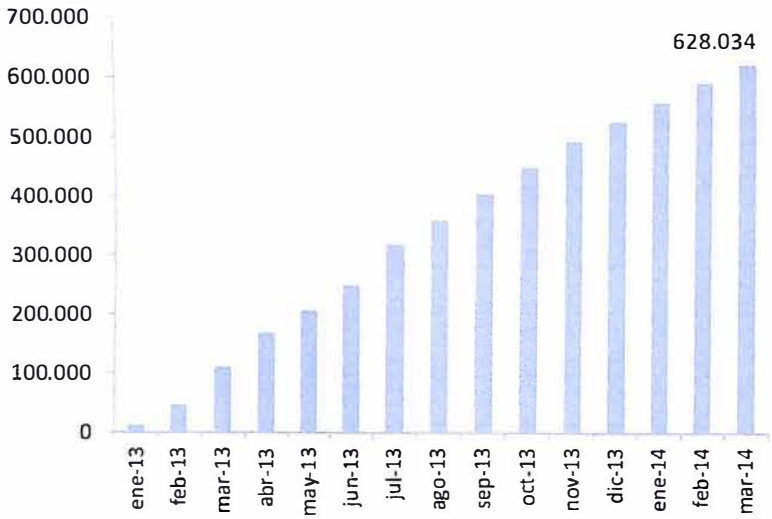
Como el uso de esta moneda no es centralizada, no impone límites cuando se realizan las transacciones ni nos agregan comisiones, aunque un cierto porcentaje de fraude es aceptado como algo inevitable; la idea es que todo en cuanto al comercio, trabaje con esta moneda, pero como al inicio de todo debe adaptarse es por ello que este dinero digital tiene la posibilidad de cambiarlo por una moneda física conocida a nivel mundial como es el Dólar, Yen o Euros; en los sitios http://www.*mexbt.com* y http://www.*fxopen.com*.

El sistema con la función de cartera digital en su versión 0.6.3 es aplicada a los sistemas operativos Linux y Windows, este sistema de cartera digital permite realizar transacciones, enviar o recibir dinero digital desde cualquier parte del mundo. Las transacciones como moneda electrónica es una cadena de firmas digitales, que al momento de ser generadas se genera una clave pública que será usada hasta el final de la moneda, un beneficiario puede verificar las firmas para verificar la cadena de propiedad única no sea usada 2 veces, en fraude. Al momento de realizar las transacciones una firma electrónica es añadida y es verificada por el minero del Bitcoin y la transacción es almacenada en la red de internet. Podemos observar el esquema de funcionamiento del Bitcoin en el Anexo 7.1.

La plataforma móvil para microempresas es básicamente la banca digital personalizada ya que en este tiempo los dispositivos conectados a la web son ya casi comunes como ilustra la figura 2 donde nos muestra que para Marzo 2014 ya existían alrededor de 628.034 dispositivos móviles habilitados como carteras móviles en las que entre enero 2013 a marzo 2014 alcanzaron un importe acumulado de Bs 111 millones de bolivianos y en volumen a 885 mil operaciones de acuerdo a datos del Banco Central de Bolivia (BCB, 2014) lo que nos indica que la accesibilidad a transacciones móviles es más accesible, por ende se desarrollara una plataforma móvil para que nuestro banco baya

siempre con nosotros; existe también la cartera digital *Bitcoin wallet* la misma que se adapta para los sistemas operativos Linux y Windows en diferentes versiones.

Figura 2: Número de dispositivos móviles habilitados como billeteras móviles.



Fuente: Boletín Informativo BCB publicación mensual Nro. 4

1.2.1. Antecedentes temáticos

Como referencia temática para el tema seleccionado se encontró el proyecto realizado en Informatics Institute, University of Amsterdam las cuales hacen referencia a BTC, como por ejemplo: *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation* por Nilolei M. Kaplanov mencionado en el artículo Bitcoin: a Money-like Informational Commodity escrito por Jan A. Bergstra y Peter Weijland. (Weijland, 2014)

1.2.2. Antecedentes institucionales

Cerámicas Jiwasa es una microempresa que trabaja con cerámica decorativa, en otras palabras, barro con valor agregado. Realiza diferentes modelos como ser nacimientos, adornos de escritorio, vasijas con figuras Tihuanacotas, además denota que tiene la posibilidad de exportar obteniendo así la certificación de IVNORCA.

Actualmente la microempresa lleva sus productos al interior de país, mediante estos se alcanza al mercado internacional quienes trabajan como intermediarios.

Figura 3: Cerámica decorativa Jiwasa

Fuente: Figuras proporcionada por la microempresa.

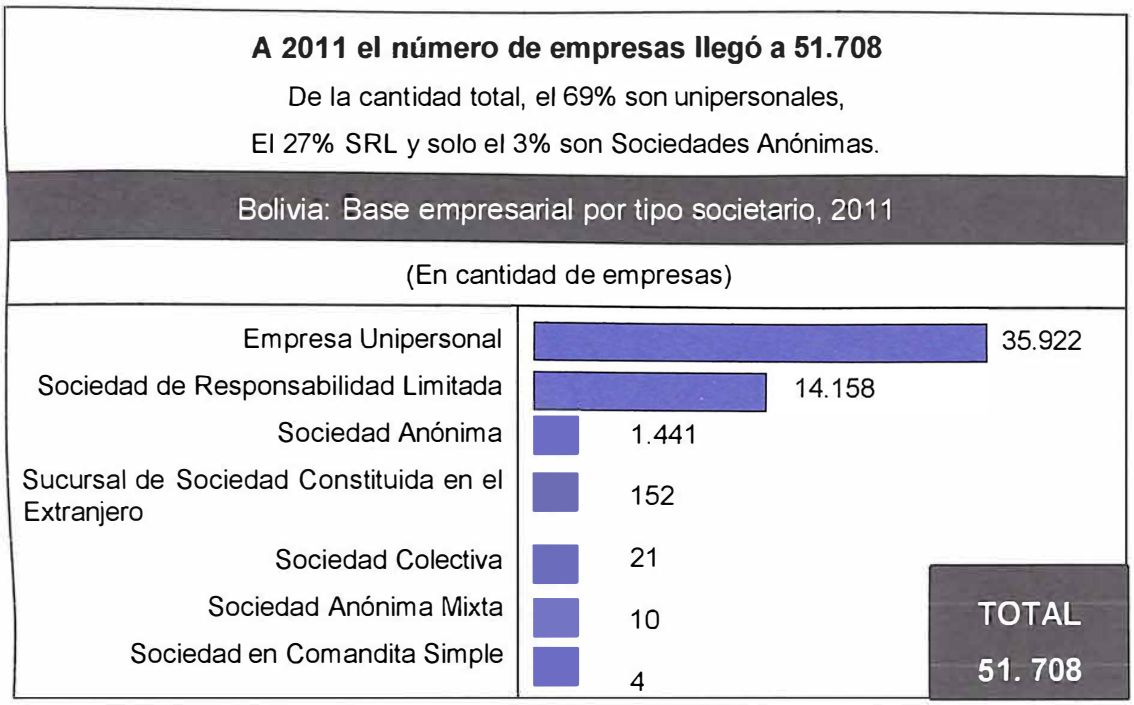
1.3. Planteamiento del Problema

Se tiene que a diciembre de 2011, de la base empresarial en el ámbito nacional que alcanza las 51.708 empresas, sólo 1.441 firmas son sociedades anónimas, lo que representa el 3%, según datos de Fundempresa. El año pasado se registraron 167 nuevas compañías de este tipo. Comparativamente, la cantidad de inscripciones en la gestión 2010 fue de 144 empresas del tipo Sociedad Anónima (empresas grandes). Esto significa que en 2011 hubo un crecimiento del 16% respecto a similar periodo del año precedente, señalan los datos de la Fundación para el Desarrollo Empresarial - Fundempresa.

Del total de la base empresarial de Bolivia a diciembre del 2011, la mayor cantidad son firmas unipersonales con 35.922 (69,4 %), le siguen las sociedades de responsabilidad limitada (SRL) 14.158 (27,4%) el resto de las sociedades llega al 187 (0,36%) (Quispe, 2012).

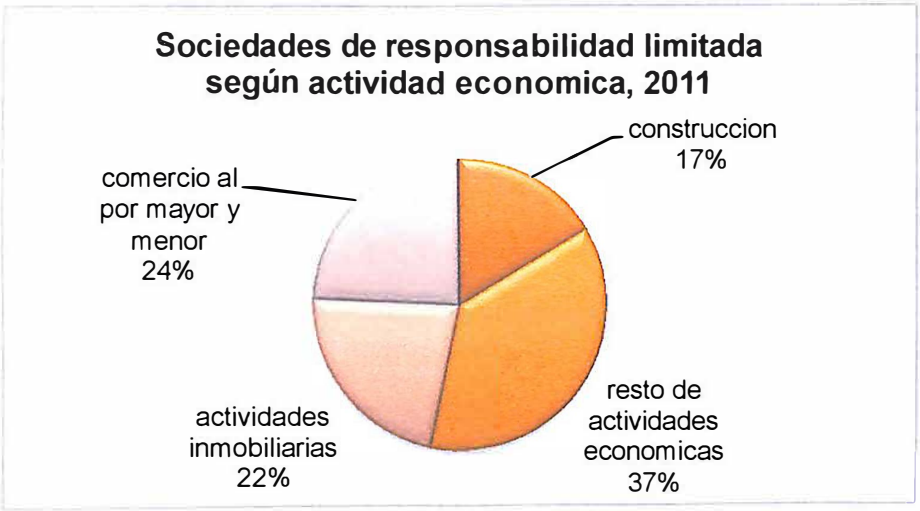
En la Figura 4 observamos que las empresas unipersonales superan el 69% del total de empresas y la figura 5 notamos que Bolivia tiene la capacidad de brindar mano de obra eficiente ya que en la misma figura observamos que el comercio al mayor y menor es un 24%, el 17% es construcción, las actividades inmobiliarias son en un 22% y el resto de las actividades económicas donde se encuentran artesanías como tejidos, cerámica decorativa, agricultura y otros en un 37% por lo que la capacidad de realizar productos de calidad, a tal punto que nuestro trabajo vale más en el exterior a comparación del mercado interno.

Figura 4: Empresas registradas en Bolivia, solo 3% son grandes



Fuente: La Razón, Economía – Quispe Aline, 2012

Figura 5: **Clasificación según actividad económica**



Fuente: La Razón, Economía – Quispe Aline, 2012

Pero una de las desventajas para un microempresario en el ámbito del comercio exterior, es que no tiene una cuenta activa en el banco, más difícilmente los requisitos para exportar su producto o las cuentas que ellos manejan son mínimas, por lo que la limitación en el acceso financiero es un problema.

De acuerdo a los datos de Fundempresa durante el año 2010 se cerraron 318 empresas de diferentes rubros, Para el ex presidente del Banco Central de Bolivia, Armando Méndez, la cifra es preocupante y demuestra que en el país no existe actividad económica que asegure la permanencia de las empresas, especialmente en el rubro de los servicios.

1.4. Formulación del Problema

La dificultad emerge al momento de realizar transacciones que van más allá de nuestras fronteras donde la divisa es diferente al Boliviano, es ahí donde necesitamos un medio el cual nos facilita la transacción, la misma que es cambiada a una divisa global en este caso el Dólar, Euro o el Yen; (conocidas a nivel mundial).

Por consiguiente debemos acudir a un tercero de confianza el cual nos permitirá hacer la transacción, pero como es una transacción, cobraran cierta comisión, esta depende de acuerdo a la entidad financiera, en la Tabla 1 a continuación mostramos los diferentes pre- requisitos para optar por alguna transacción entre estas estudiamos Banco Fie, Banco nacional de Bolivia *BNB,* Western Union, Tigo Money, electrónica PayPal.

Tabla 1: Requisitos a la apertura de cuenta para realizar transacciones

Entidad	Requisitos
Banco FIE	✓ Fotocopia de carnet ✓ Factura de luz o agua. ✓ Croquis de domicilio.
Tigo money (P2P)	Tener activa una línea activa de Tigo, y plenamente con registro de numero; y para ello: ✓ Carnet de identidad
Western Union	La persona debe llenar un formulario al momento de enviar el dinero y para que la transacción sea recogida la persona debe contar con un documento de acreditación.
PayPal	✓ Ser residente de uno de los países que aparecen en la página.(https://www.paypal.com/es/webapps/mpp/country-worldwide) Para obtener un Estado verificado, es necesario: ✓ Añadir una tarjeta de crédito y completar el Programa de uso ampliado.

Fuente: Elaborado en base a datos proporcionados en línea por la entidades financieras.

La dificultad se debe a la existencia de intermediarios financieros, los mismos que cobran comisiones, a veces muy altas. Además el Boliviano es una moneda local y para realizar negocios en la región o en el mercado global se hace necesario el uso de otras divisas y de nuevo se cae en costos adicionales, aun así para acceder a estos servicios los requisitos exigidos por la banca

suelen ser inalcanzables para los microempresarios y de esta manera pierden competitividad.

Es por eso que se pudo identificar como el problema principal: la dificultad en el acceso a las transacciones financieras para las microempresas.

1.5. Fin y propósito

El propósito es expandir el uso del dinero digital Bitcoin, debido a las diferentes ventajas que nos trae el simple hecho de usar dicha moneda para la microempresa Jiwasa, con el fin de tener mayores facilidades de acceso al mercado global.

1.6. Objetivos

1.6.1. Objetivo General

"Desarrollar un prototipo que utilice los atributos de la cartera móvil digital Bitcoin dirigida a la facilitación de transacciones financieras para microempresas bolivianas, orientado en particular a la microempresa de cerámica Jiwasa".

En este punto encontramos relación de lo que es la aceptación de la tecnología móvil, por lo que encontramos como una solución a la dificultad de acceso a las transacciones, llevar el banco donde sea necesario es una manera de acortar procesos y acortar comisiones.

1.6.2. Objetivos Específicos

Implementar el prototipo en el comercio electrónico dirigida a la facilitación de transacciones financieras.

Realizar un módulo de seguimiento de la economía Bitcoin para mantener informado a su operador.

- Precio de Bitcoin.
- Transacciones recientes.

Realizar el módulo de productos donde se tengan todos los productos de la microempresa.

Realizar el módulo Carrito donde se tiene los detalles de los productos que se seleccionaron para que posteriormente sean comprados.

Además se realiza el módulo de contactos donde el cliente podrá contactarse con el proveedor.

1.7. Justificaciones

1.7.1. Justificación Teórica

La cartera móvil digital pretende ser un espacio dinámico para el usuario, donde la información del Bitcoin esté al alcance del usuario.

Al realizar las transacciones nos centramos en el área de las transacciones mediante la red internet donde se pretende definir conceptos necesarios y óptimos para el desarrollo del proyecto.

1.7.2. Justificación Metodológica

Se usará la metodología RUP ya que nos ayuda a realizar el análisis, diseño, implementación y documentación del sistema además enfrentar con coraje los diferentes cambios que se mostraran en el transcurso de los cambios de acuerdo a la economía Bitcoin.

1.7.3. Justificación Práctica

El dinero en efectivo causa ciertas susceptibilidades de la originalidad, el estado del billete. Por esta razón es importante proporcionar este modelo que permita aprovechar en la red de internet y monedas digitales como medio de comunicación en la transacción; lo que funciona como una cartera móvil al momento de realizar compras o al guardar tu dinero.

1.7.4. Justificación Social

Las perdidas sustanciales ocasionadas al cliente a causa de los intereses o comisiones generados por un banco, es la causa por la que algunos microempresarios no trabajan con entidades financieras lo que impide el crecimiento como microempresa. Por esta razón se plantea trabajar con la moneda digital Bitcoin ya que no trabaja con intermediarios lo que para la sociedad implica menos comisiones al momento de realizar alguna transacción.

1.7.5. Justificación Económica

El trabajar con una nueva moneda digital descentralizada es reducir costos en las transacciones, además ya que no requiere prerrequisitos o limites

arbitrarios para trabajar con esta moneda permitirá abrir una cuenta en el mismo equipo (computadora o celular).

1.8. Límites, alcances y aportes

1.8.1. Límites

- ✓ Solo se consideran costos del producto ofrecido por los microempresarios directos y no así los costos que incurre la exportación por la escasa importancia que tiene en el área de objeto de estudio.
- ✓ El sistema únicamente procesara pagos con la moneda digital bitcoin.

1.8.2. Alcances

La aplicación permite saber al usuario el precio del Bitcoin en bolivianos.

Se tomaran en cuenta microempresas unipersonales de acuerdo a Datos del año 2011, debido a que son las últimas estadísticas a la fecha.

Esta investigación sólo tomará en cuenta el estudio y análisis de la información referente al problema transaccional en los microempresarios, tomando en consideración aquellos elementos que aporten criterios con los cuales se puedan realizar juicios valorativos respecto al papel que juega las transacciones financieras.

1.8.3. Aportes

- ✓ El estudio de una nueva moneda digital para el comercio no gubernamental.
- ✓ Un modelo de transacción con dinero digital Bitcoin.
- ✓ El inicio a una nueva forma de pago.

1.9. Modelos y Herramientas

A. Herramienta de modelado

UML, (Unified Modeling Languaje) lenguaje de modelado de sistema del software es grafico que permite construir, visualizar y documentar un sistema de software. Para este modelo se utilizara la versión 2.0

B. Herramienta de modelado

Metodología de desarrollo RUP esta metodología nos ayudara a realizar el análisis, diseño, implementación y documentación de sistemas.

Herramientas

Enterprise architect 7.5, herramienta que permitirá desarrollar los diagramas UML.

Microsoft office Project 2007, herramienta que nos permitirá realizar cronogramas de los diagramas Gantt.

Java, lenguaje de programación.

Eclipse, ambiente de trabajo.

Microsoft office Excel 2007, herramienta permitirá realizar graficas estadísticas que se incluirán en el presente proyecto de grado.

Minero de bitcoin 0.6.3, herramienta que le funcionara para la realización de transacciones de una cartera a otra.

2. MARCO TEÓRICO

2.1. El dinero

El dinero es el medio de pago, es decir las monedas, los billetes y los cheques que utilizamos cuando compramos cosas.

Figura 6: Principales sistemas por los cuales se moviliza el dinero electrónico y cheques en Bolivia

Fuente: Boletín Informativo BCB publicación mensual Nro. 4

SIPAV, administrado por el BCB mediante el cual se realizan pagos entre las entidades financieras.

SPT, medio por el cual el sector publico realiza pagos electrónicos.

Liquidación de títulos valores descentralizados administrado por la Empresa de Depósitos de Valores EDV.

ACH y CCC, cámara de compensación de pagos electrónico y cheques.

Sistema de pagos transfronterizos, por el cual los fondos son enviados y recibidos del/al exterior.

Billetera móvil utilizado desde los dispositivos móviles.

Samuelson indica que el dinero es más que eso, el dinero es un lubricante que facilita los intercambios. Cuando todo el mundo confía en él y lo acepta en concepto de pago de bienes y deudas, se facilita el comercio. Imaginemos lo complicada que sería la vida económica si tuviéramos que trocar bienes por bienes cada vez que quisiéramos comprar una pizza o ir un concierto. ¿Qué servicios podríamos ofrecer a la pizzería? ¿Y qué decir de nuestra educación? ¿Qué podríamos trocar con nuestra universidad por las tasas de matrícula que necesita? Dado que todo el mundo acepta el dinero como medio de cambio, se simplifica enormemente la necesidad de emparejar las ofertas y las demandas.

Los gobiernos controlan la oferta del dinero a través de sus bancos centrales. Pero el dinero, al igual que otros lubricantes, puede recalentarse y dañar el motor económico. Puede descontrolarse y provocar una hiperinflación, en la que los precios suben muy deprisa. Cuando eso ocurre, la gente se dedica a gastar su dinero rápidamente, antes de que pierda valor, en lugar de invertirlo para el futuro. Eso es lo que sucedió en varios países latinoamericanos en la década de 1980 y en muchas antiguas economías socialistas en la de 1990, periodo en que las tasas anuales de inflación superaron el 1.000 o incluso el

10.000 por 100. Imagínese el lector que recibe la nómina y que el fin de semana está ya ha perdido un 20 por 100 de su valor". (Samuelson, 2002)

2.2. Historia del dinero

Este punto se desarrollará fundamentalmente haciendo referencia al trabajo de Weatherford (1997) que en resumen relata:

Cuando comenzó el intercambio de productos con fin de variar los productos que tenían, por ende los romanos pagaban y compraban con sal; es entonces el origen de la palabra salario; comenzaron a pagarse con el medio más escaso que existía en este entonces, la sal; medio con el que se realizaban compras, en Grecia surgió la frase "no vale su sal" ya que la compra era con cualquier producto excepto la sal es por eso que viene el origen de las monedas.

En Mesopotamia, a China, Egipto y otros muchos lugares del mundo antiguo pueden hallarse elementos parecidos al dinero e instancias parecidas al mercado pero en rigor, en ninguno de ellos se utilizó verdaderamente la moneda hasta el surgimiento de Lidia y el subsiguiente acuña miento de la primeras monedas, ocurrió entre 640 y el 630 a. C. el genio de los monarcas lidio consintió en reconocer la necesidad de lingotes muy pequeños y fácilmente transportables, equivalentes a no más de unos pocos días de labor o una pequeña fracción de una cosecha. Al confeccionarse los lingotes más reducidos, de un tamaño y peso estándar, y al imprimir en ellos un emblema que indicaba su valor incluso a los analfabetos, los reyes de Lidia ampliaron exponencial mente las posibilidades de cualquier empresa comercial.

Las primeras monedas que confeccionaron fueron las electro, una aleación de de oro y plata de color ámbar que se da en la naturaleza. Convertían el electro en fichas ovaladas, varias veces más gruesas que las

monedas actuales equivalentes en tamaño al tercio superior de un dedo pulgar adulto. Para garantizar su autenticidad, el rey hacia estampar en cada una de ellas su emblema, una cabeza de león. El proceso de estampar el sello aplanaba las unidades, iniciando de ese modo su transición desde un trocito ovalado a una moneda plana y circulas como las actuales. (Weatherford, 1997)

Al elaborar los trocitos del mismo peso y, por ende, de aproximadamente del mismo tamaño, el rey eliminaba una de las fases más engorrosas del comercio: la necesidad de pesar el oro cada vez, en cualquier transaccional que se hacía. De ahora en adelante, los mercaderes podían estimar el valor a simple vista o bien contabilizar el número de monedas. Esa estandarizan redujo en buena medida la posibilidad de hacer trampas con la cantidad o la calidad del oro y la plata en cualquier intercambio. Uno no precisaba ser un experto en el manejo de una escala o en el arte de valorar la pureza del metal para adquirir una cesta de trigo, una par de sandalias o un ánfora de aceite de oliva. El empleo de monedas que habían sido pesadas y estampadas con un sello en el taller real hacia posible que el comercio fluyera más rápida y más honestamente y le permitió a la gente participar incluso si no disponía de medidas. El comercio con monedas abrió nuevas posibilidades a nuevos segmentos de la población.

La acuñación de moneda dio gran ímpetu al comercio, al proveerlo de una estabilidad dela que antes había carecido. Las monedas se convirtieron, de modo literal, en una base con la cual se comparaban otras mercancías y servicios que ahora podían medirse y venderse con mayor facilidad. La moneda brindo a los antiguos comerciantes, granjeros y consumidores un medio de intercambio permanente que era fácil de almacenar y transportar. Esa facilidad de uso, la estandarizan del valor de su duración como reserva para almacenar la riqueza familiar atrajo cada vez más gente hacia la nueva mercancía. (Weatherford, 1997)

"...el uso del dinero no requiere de la interacción cara a cara y las relaciones intensivas de un sistema basado en el parentesco. Ni requiere de sistemas administrativos, policíacos y militares de basto alcance. El dinero se volvió el nexo capaz de relacionar a los seres humanos en bastantes mas formas dela que antes era posible, sin aportar cuan distante o transitorias fueran estas relaciones. El dinero comunicaba a los individuos de una forma mucho más vasta y eficaz que cualquier otro recurso humano". (Weatherford, 1997)

Por lo que cabe recalcar que el dinero es sinonimo de confianza en que ese medio tiene valor determinado, al momento de realizar alguna compra, o se adquiere en funcion de deuda para el que lo adquiere viene a ser como parte de una adquicicion en materia o servisio y el vendedor debe confiar a que el acreedor pagara, por ende se tiene como factor de credibilidad a un medio de confianza.

2.2.1. Evolución de medios de pago

De acuerdo a la historia según el seminario realizado en instalaciones de la UNIFRAZ por representante del Banco Central de Bolivia, en dicho seminario nos indicó el siguiente orden en la evolución de medios de pago.

- El trueque
- Dinero mercadería (peso y volumen)
- Artefactos de metal (500 A.C.) y monedas (700 A.C.)
- Papel moneda
- Primeros bancos Exigían órdenes de pago verbales y con testigos (Europa, siglo 13)

- Primeros billetes emitidos por el Banco de Inglaterra (1694)
- Primera cámara de compensación de cheques (Londres, 1773)
- Primera tarjeta de crédito (EE.UU. 1920)
- Creación del primer Banco Central de Bolivia como único emisor de moneda (1925)
- Compensación entre tarjetas de crédito (EE.UU. 1938)
- Primer registro contable electrónico (Computadora General Electric "ERMA" EE.UU. 1955)
- Cheques con impresión de número de cuenta utilizando caracteres estandarizados "MICR" Reconocimiento de Caracteres por Tinta Magnética para permitir el procesamiento electrónico de graves volúmenes de documentos (EE.UU. 1955)
- Primer ATM – Modo de Transferencia Asíncrona (EE.UU.1968)
- Sistema de transferencia de fondos interconectado 239 Bancos (Bélgica, 1973), hoy 10,000 entidades y 20 MM de transferencias diarias.

2.3. Dinero fiduciario

El dinero llamado fiduciario es el que se basa en la fe o confianza de la comunidad, es decir, que no se respalda por metales preciosos ni nada que no sea una promesa de pago por parte de la entidad emisora. Es el modelo monetario que manejamos actualmente en el mundo, incluyendo el dólar estadounidense, el euro y todas las otras monedas de reserva. Esta tendencia

comenzó con el Nixon Shock de 1971 (aunque es original del siglo XI en China, y responsable de la expansión de las dinastías Yuan y Ming), que terminó con el respaldo en metales preciosos del dólar norteamericano, iniciándose también con ello la fluctuación de las divisas, que basan su valor en relación al valor de las demás, y con ello el altamente voluble y lucrativo mercado de divisas, que mueve alrededor de 3 billones de dólares al día. Las monedas y billetes fiduciarios no basan su valor en la existencia de una contrapartida en oro, plata o cualquier otro metal noble o valores, ni en su valor intrínseco, sino simplemente en su declaración como dinero por el Estado y también en el crédito y la confianza (la fe en su futura aceptación) que inspira. Sin esta declaración, la moneda no tendría ningún valor: el dinero fiduciario sería entonces tan poco valioso como el pedazo de papel en el que está impreso. (Fiduciario, 2012)

Un billete actual es una clara representación de dinero fiduciario, por cuanto objetivamente considerado carece de valor. Su valoración viene dada por la autoridad monetaria que lo emitió, que goza de confianza entre los sujetos que la aceptan.

Ahora si bien se sabe que el dinero es simbolo de confianza y muestra de ello son las diferentes medidas de seguridad impuestas por el estado, de tal forma que no sea suseptible a fraude, pero ademas se debe tomar en cuenta que cierta suseptibilidad a fraude siempre es aceptable; una de otras alternativas es el dinero digital.

Como crean los bancos el dinero (y poder) según Juan Torrez Lopez (2009) el dinero bancario es otro invento de los bancos ya que lo que ellos adoptan es prestar dinero a una tasa de interez por donde generan una comicion; por ejemplo si se tiene Bs. 100 depositados y otro sujeto pide prestado Bs. 20 entonces en el transcurso del año generan dinero de los intereses, donde ya

hay un cierto monto de dinero generado o si por lo contrario no se paga lo que se presto entonces el banco se queda con lo que el prestatario dejo como garantia, generando asi dinero de la garantia. Dinero bancario el dienro creado por el interez de los difrentes prestamos es ese el dienro bancario. (Lopez, 2009)

Haciendo asi un negosio un tanto incomodo para el microempresario que si no puede optar por un microcredito peor aun por alguna transaccion desde otro lugar del mundo lo que le imposibilita el comercio hacia el exterior, es por eso que ahora se toma en cuenta el dinero digital.

2.2. Teoría cuantitativa del dinero

Hasta ahora he considerado al dinero como un factor neutro en la formación de precios sin embargo vamos a ver cómo eso no es así. Vamos a ver primero algunas definiciones (dentro de la Teoría Cuantitativa del Dinero).

La cantidad de dinero (M): el conjunto de billetes y monedas de curso legal.

Velocidad de circulación del dinero (V).

Número de veces que el dinero cambia de dueño en la realización de compras por consumidores finales en un determinado periodo de tiempo (un año).

Nivel de Precios (NP): valor de un conjunto de bienes que se considera representativos del consumo de una población.

Producción (P): Número del conjunto de bienes que se considera representativos del consumo de una población que se producen en un año. (Obsérvese que por producción no se trata del conjunto de bienes que se producen en general sino del número de un conjunto de unos determinados bienes en una determinada proporción que es la que se considera representativa del consumo de una población y que es el mismo que se utiliza en el nivel de precios). A partir de estos factores la Teoría Cuantitativa del Dinero dice simplemente que: La cantidad de dinero por su velocidad de circulación es igual al nivel de precios por la producción.

$$M \times V = NP \times P$$

Esta igualdad, siempre claro está que todo lo producido sea vendido, es autoevidente. Si M es la cantidad de dinero y V la cantidad de veces que cambia de circulación (en la compra de productos finales) entonces M x V es igual al valor de todos los bienes finales vendidos.

Nos dice que si P es el conjunto de bienes producidos y NP es el valor de cada uno de esos conjuntos entonces P x NP (siempre que todo se venda) es igual al valor de todos los bienes finales vendidos. Basados en esta verdad autoevidente vamos a analizar lo que pasaría si cambia alguno de los factores.

Vamos inicialmente a considerar V como una constante. Parece algo plausible dado que la gente suele cobrar sus salarios en periodos de tiempo estables (semanales, mensuales) y los beneficios de los capitalistas también tienden a ser regulares (aunque puedan variar en determinadas épocas del año) y la parte del dinero que dedica la gente a comprar (y por tanto lo que ahorra) es también estable. Hasta ahora habíamos considerado al dinero como algo neutro es decir que su cantidad era constante. Por tanto habíamos considerado una parte de la ecuación (M x V) como una constante, en

consecuencia el otro lado de la ecuación también tenía que ser una constante. Y efectivamente era así:
Si P, la producción, aumentaba, es decir si la oferta aumentaba entonces los precios (NP) debían de bajar para que se mantuviese una cantidad constante. Y viceversa si P, la oferta, disminuía entonces los precios (NP) tenían que subir.

Pero vamos a ver qué pasa si M deja de ser una constante, es decir si el dinero deja de ser un factor neutro.

Aumento de la cantidad de dinero: Si la cantidad de dinero aumenta entonces todo cambia en el otro lado de la ecuación. Un aumento de la oferta ya no significa necesariamente una bajada de precios es más con frecuencia sucede que la producción aumenta y el nivel de precios también. Esto es especialmente grave pues la gente deja de percibir una relación clara entre el aumento de la producción y los precios. De acuerdo a la pagina en linea (http://www.desdeelexilio.com/2012/06/04/comprendiendo-la economia-capitulo-16-la-teoria-cuantitativa-del-dinero/, 2012)

Casi todos los economistas están en favor de un aumento continuado de la cantidad de dinero para no caer en la terrorífica, según ellos, deflación. La deflación supone, según la ortodoxia económica imperante, un descenso de la demanda y la entrada en una espiral de bajadas de precios y descenso de la demanda que llevaría a una depresión. ¿Es esto necesariamente así?

El aumento de la producción con una cantidad de dinero constante no lleva a una depresión.

La producción puede aumentar por dos razones: porque aumentan los factores de producción: se emplean a más trabajadores o por un aumento de la productividad: con el mismo número de trabajadores se produce más.

En el primer caso las empresas contratarán a más trabajadores pero como la cantidad de dinero es la misma sólo podrán hacerlo pagando menos a cada trabajador. Sin embargo a la hora de vender, al aumentar la oferta, deberá, y podrá dado que ha pagado menos a sus trabajadores, bajar sus precios. El resultado: salarios más bajos, precios más bajos e igualdad de poder adquisitivo para el trabajador.

En el segundo caso, si la empresa produce más con el mismo número de trabajadores, la empresa podrá, y deberá, bajar sus precios. Lo que sucede entonces es que los salarios permanecen constantes pero al bajar los precios el poder adquisitivo de los trabajadores aumentará.

Dado que la productividad suele aumentar con el tiempo:

¿No aplazará la gente de modo indefinido sus decisiones de compra a la espera de precios más bajos?

No, la gente compra cuando tiene necesidades que satisfacer, es posible que aplace alguna decisión de compra a la espera de mejores precios, pero lo que no puede hacer es aplazar todas sus compras de manera indefinida puesto que entonces nunca satisfacerla sus necesidades. Por otro lado la bajada de precios hace que la gente pueda satisfacer necesidades que antes no podía satisfacer y es muy probable que ante la posibilidad de satisfacerlas haga sus compras (de nuevos productos) de manera inmediata.

En cualquier caso lo que se producirá, y además en corto plazo, es que la gente se habituará a una lenta mejora de su poder adquisitivo a lo largo del tiempo. Quizá el mejor ejemplo, aunque no me gusta acudir a los ejemplos, sea el mercado de ordenadores. Los ordenadores llevan bajando su precio y/o mejorando sus prestaciones desde hace décadas y la gente no aplaza por ello sus compras.

¿No disminuirán la oferta las empresas debido a la bajada continua de los precios?

Las empresas bajan sus precios porque sus costes son menores no porque la demanda haya disminuido. Es más al bajar los precios la demanda aumentará y por tanto las empresas aumentarán su oferta. Lo importante es que mientras que la bajada de precios responda a un descenso de los costes los beneficios por unidad producida no van a disminuir, es más van a aumentar en la media que aumente la productividad, y por tanto las empresas van a tener fuertes incentivos en producir más.

¿Y si las empresas mantienen los precios y la oferta y en cambio lo que hacen es despedir a trabajadores dado que la productividad ha aumentado? En un mercado libre, y en consecuencia con competencia, si las empresas deciden mantener sus precios y prescindir de trabajadores va a haber un fuerte incentivo para la primera empresa que decida bajar sus precios porque podrá echar a la competencia del mercado y también va a haber un fuerte incentivo para producir más y emplear a más trabajadores por la misma razón que exponía en la segunda cuestión. Se puede argumentar que al haber más trabajadores en paro, debido a que las empresas han prescindido de ellos al aumentar la productividad, entonces la demanda disminuirá pero eso es una razón más para

que las empresas bajen sus precios: la primera que lo haga se pude hacer con el mercado.

Lo importante es que mientras que la productividad aumente las empresas siempre podrán bajar sus precios manteniendo o aumentando sus beneficios por unidad producida. Y bajar los precios es todo lo que se necesita para que la demanda aumente y con ella la producción y el empleo. La consecuencia es que un aumento de la productividad nunca va a producir una espiral de desempleo y baja demanda sino exactamente lo contrario. Aumento de la cantidad de dinero sin aumento de la productividad.

El principal argumento a favor del aumento de la cantidad de dinero es que, cuando se está en una situación de depresión o de paro elevado, dicho aumento provocará un aumento de la demanda y una disminución del número de parados y el fin de la depresión. Este argumento es la esencia del keynesianismo (es el análisis de las causas y consecuencias de las variaciones de la demanda agregada y sus relaciones con el nivel de empleo y de ingresos).

Cuando se produce una situación de depresión y de elevado paro puede ser debida a dos razones:

- Las empresas (o los capitalistas) no obtienen beneficios de sus inversiones.
- Las empresas (o los capitalistas) no saben en qué invertir su capital.

Al aumentar la cantidad de dinero aumentará la demanda y las empresas podrán subir sus precios y aumentar sus beneficios y con ello emplear a más gente que a su vez aumentará la demanda.

Esta explicación es muy popular porque se hace en tres líneas y es muy elegante. El problema de aumentar la cantidad de dinero es que al aumentar los precios los trabajadores pedirán aumentos de sueldo y entonces los beneficios de las empresas volverán a desaparecer. El argumento que se usa es simple y llanamente que los trabajadores no pedirán aumentos de sueldo, y en consecuencia aceptarán que su poder adquisitivo disminuya (dado que los precios aumentan) sin hacer nada. Este argumento es muy bueno, se llama "ilusión monetaria" y sostiene que mientras que los salarios nominales se mantengan a los trabajadores no les importará demasiado la subida de precios siempre que mantengan su puesto de trabajo. (desdeelexilio, 2012)

Pero, si los trabajadores aceptan una disminución de su poder adquisitivo, ¿no sería más fácil bajar los salarios para que las empresas vuelvan a tener beneficios y así tener incentivos para contratar nuevos trabajadores? En ese caso no sería necesario un aumento de la cantidad de dinero.

Puede parecer que las dos soluciones tienen muy parecidas consecuencias y sin embargo no es así. Aumentar la cantidad de dinero sólo se puede hacer creando una demanda artificial, gastando dinero creado de la nada en algo. Pero los trabajadores y/o las empresas que utilicen ese dinero "extra" ¡Van a demandar productos que no han sido producidos! En efecto los trabajadores y/o las empresas que van a gastar el dinero extra produciendo lo que sea no van a aumentar la producción de lo que realmente necesitan y por supuesto no van a aumentar lo ya producido. Lo que se sucederá a continuación es un exceso de demanda y la inevitable subida de precios. Como consecuencia de la subida de precios los trabajadores, siempre que sus salarios se mantengan constantes, perderán poder adquisitivo.

Pero la subida de precios no va a ser uniforme. Aunque haya considerado que la gente consume uniformemente un conjunto de bienes en la misma proporción cuando los precios cambian también cambia esa proporción. La razón es muy sencilla, aunque la satisfacción marginal de todos los productos que consumimos es similar, la satisfacción marginal se refiere a la última unidad del producto que consumimos pero no a la de los demás. En el momento que debemos de dejar de consumir varias unidades de varios productos la satisfacción marginal de cada uno de ellos va a variar de forma diferente. La consecuencia es que los precios que estaremos dispuestos a pagar por cada uno de ellos van a variar también de forma también diferente.
Si consumimos patatas y camisas y tenemos que prescindir de varias unidades de ambos productos lo más probable es que prefiramos prescindir de más camisas y menos patatas y por tanto estaremos dispuestos a pagar más por las patatas y prescindir de menos patatas y pagar menos por las camisas y prescindir de alguna camisa.

El caso es que el aumento de la demanda no va a producir una subida de precios uniforme sino que va a distorsionar el sistema de precios. Algunos productos subirán mucho de precio otros no tanto, incluso es posible que alguno baje su precio. Y lo que es muy importante: al disminuir el poder adquisitivo de la gente habrá productos que ya no podrá comprar, empresas que quebrarán y trabajadores que irán al paro.

Al final cuando el dinero salido de la nada se acabe, y los trabajadores que se dedicaban a producir lo que fuera que produjesen dejasen de hacerlo, estaremos ante una nueva cantidad de dinero. Dependiendo de la cantidad y del tiempo que se esté introduciendo dinero creado de la nada mayor será la

distorsión en los precios. Lo cierto es que dado que siempre se va a producir una demanda de bienes que no han sido producidos los precios (en su inmensa mayoría) van a subir.

Las subidas de precios van a provocar que las empresas produzcan más bienes y contraten a más trabajadores, sin embargo hay que tener en cuenta que se va a producir un reajuste dado que como dije más arriba la gente va a cambiar su patrón de consumo al perder poder adquisitivo, y en consecuencia también habrá empresas que cierren y que los trabajadores pierdan su empleo. Existe además otro problema, ante la pérdida de poder adquisitivo los trabajadores puede que dediquen menos dinero al ahorro, y así mantener su nivel de vida, con la consecuencia de que habrá menos dinero para inversiones

El aumento de la cantidad de dinero no es seguro que disminuya el paro, producirá inicialmente una disminución del poder adquisitivo de los trabajadores y una reestructuración del sistema productivo, a medio plazo si la gente no mantiene la "ilusión monetaria" puede volverse en algo estéril.

Queda la propuesta de elevar la cantidad de dinero en la misma cantidad que la producción para así mantener los precios estables. Sin embargo siempre será difícil saber cuánto va a aumentar la producción y también está el problema de hacer llegar a la gente esa mayor cantidad de dinero de forma que no haya ganadores ni perdedores.

2.3. Dinero digital

El dinero digital es anónimo e identificado es amplio, y difícil de definir en un medio tan extenso como el de los medios de pago electrónicos (EPS). A

todos los efectos se definirá el dinero digital como aquel dinero creado, cambiado y gastado de forma electrónica. Este dinero tiene un equivalente directo en el mundo real: la moneda. El dinero electrónico se usará para pequeños pagos. El dinero electrónico puede clasificarse en dos tipos:

- Dinero on-line: Exige interactuar con el banco (vía módem o red) para llevar a cabo una transacción con una tercera parte.
- Dinero offline: Se dispone del dinero en el propio ordenador, y puede gastarse cuando se desee, sin necesidad de contactar para ello con un banco. Estos sistemas de dinero electrónico permiten al cliente depositar dinero en una cuenta y luego usar ese dinero para comprar cosas en Internet.

Las monedas virtuales están en el punto de vista del mundo desde que Facebook lanzó los Facebook credits, que se pueden utilizar para comprar cosas en Facebook. Por ejemplo alquilar una película u objetos virtuales. La idea es que en el futuro pudiéramos utilizar esas monedas para comprar bienes físicos que nos traen a casa. No obstante, tengamos en cuenta que si al final lo que sucede es que unos Facebook credits son dólares a un tipo de cambio fijo, los créditos de Facebook no dejan de ser dólares. Es como el dinero que se compra y se puede utilizar única y exclusivamente dentro de un parque de atracciones. En Second Life también existía una moneda equivalente. (Navarro, 2011)

Según el punto de vista de Navarro (2011) lo interesante es cuando esa moneda no tiene nada que ver con otra moneda generada por un banco central, como son los dólares, los euros o los reales brasileños. La forma en la que en principio se le ocurre hacer esto es tener una moneda pegada a una mercancía por ejemplo el oro.

Claro que eso depende de su reputación para no emitir más de lo que tiene en reservas de oro. Donde se dice oro podemos poner plata, diamantes, petróleo, granos de cacao o cualquier cosa que aceptemos que tenga valor. La diferencia con Bitcoin que se propone es que Bitcoin no son más que archivos de ordenador. Estos se pueden crear en un ordenador. Donde existen mercados en los que se intercambias Bitcoin por divisas reales (como yenes o libras).

Y la interrogante que surge es: ¿Eso es completamente seguro? ¿Seguro que no se pueden crear fácilmente esas monedas? Porque si llega alguien en cualquier rincón del mundo y consigue crear más monedas de lo esperado creo que la hemos fastidiado. Si algo tiene valor para ser hackeado es muy probable que alguien lo acabe consiguiendo.

2.3.1. Facebook credits

Las crisis son puntos de inflexión que anticipan un cambio. Cuanta más crítica es la situación más revolucionaria es la respuesta que surge de los afectados nos dice Mexía (2009) el infarto sufrido por el sistema financiero internacional, que ha quedado al borde del coma, es un campo de cultivo idóneo para el surgimiento de nuevas formas pago, de una nueva economía sin reservas federales ni bancos centrales. Llega el momento de las divisas virtuales.

Hasta ahora el dinero siempre ha tenido una forma física, aunque sea como tarjeta de plástico con banda magnética, pero nos encontramos a las puertas del "boom" del billete que no se puede tocar creado a través de las populares redes sociales. El fenómeno no es nuevo pero sí disperso. Plataformas como Hi5 tiene ya su Hi5 Coins, mundos de videojuego como

"Second Life" cuentan con sus Linden Dollars y en Twitter surgieron los poco conocidos Twollars. Meros ejemplos de una larga lista de "dineros" aceptados en el llamado ecosistema virtual que, sin embargo, no interactúan entre ellos. Vamos, no se han establecidos los tipos de cambio para estas "divisas".

Compañías como Spare Change o Jambool (con su SocialGold) han intentado llenar ese hueco y ofrecen el cambio de moneda real por moneda digital que es aceptada para operaciones en centenares de juegos y redes sociales como MySpace. Un paso intermedio hacia la creación de un sistema monetario digital universal. No obstante, la cristalización de estas nuevas formas de pago necesitará del liderazgo de la figura dominante del "networking". Admeas Mexía nos dice que más de 200 millones de usuarios en todo el mundo convierten a este sistema de comunicación en la mejor vía para naturalizar la aceptación de una divisa que pueda cuajar más allá de la propia red y sea aceptada como valor fiable en transacciones ordinarias, como contratar un crucero por el Caribe, hacer la compra por internet, o adquirir unas entradas para un concierto. Estos pueden canjear sus ingresos en "moneda" Facebook a dólares, por poner un ejemplo, pero puede que en el futuro prefieran mantener las divisas virtuales. La "magia" económica comenzaría a producirse cuando ese dinero digital fuese ampliamente aceptado con la confianza de que en cualquier momento uno puede cambiarlo en billetes reales. En ese momento ya no habría estrés para canjear las divisas ¿qué más da una que otra si valen todas? Un paso que requeriría un tipo de cambio "Facebook – dólar- euro" (por ejemplo). A partir de ahí, no habría diferencias aparentes en el funcionamiento económico. Las compras por internet son ampliamente aceptadas a día de hoy; superadas las dudas iniciales, quien más o quien menos ha usado su número de tarjeta alguna vez para adquirir algo a través de la red. Es el pan nuestro de cada día. Con la moneda digital sería igual, pero en vez de respaldar la compra

el sistema bancario lo haría Facebook, o en su caso una red de entidades generadoras de crédito digital que podría incluir también a MySpace, Hi5, así como productores de videojuegos "online".

Es más, podría llegarse a la producción de tarjetas con dinero digital para pagar en establecimientos, igual que se hace con el dinero conocido. Los más ricos en esas divisas podrían a su vez dar créditos con intereses a usuarios de internet sin necesitarse una mediación vía dólar o euro. Comenzaría la especulación virtual, la creación de "millonarios de divisas de internet" y también de pobres de la red, que como consecuencia lo serían también en la vida real. Igual que ocurre en un casino cuando uno cambia su dinero por fichas, pero el casino sería global y las fichas imaginarias.

Una de las más comprometedoras divisas digitales para el futuro era la divisa de facebook credit ya que como se indicaba anteriormente es la que mediante esa red social está al alcance de gran parte del mundo, pero como se indicó que facebook abandona su moneda virtual. La red social Facebook ha decidido terminar con su propio sistema de crédito para pagos online que fue adoptado en el año 2009, y sustituirlo por el empleo de monedas reales y una nueva opción de pagos por suscripción. Prashant Fuloria, director de Gestión de Producto de Facebook, ha indicado que la medida se ha adoptado tras observar como la mayoría de los juegos presentes en la red social han implementado sus propias monedas virtuales. El dirigente añade que a partir de ahora si se desea pagar desde Facebook se podrá hacer en la moneda local de cada país. La medida ya ha empezado a implantarse en algunos juegos y aplicaciones que ofrecen contenidos de pago y para finales de año deberá estar presente en todos ellos nos dice Domenech (2012).

El largo proceso acababa con muchas compras de las llamadas "impulsivas". Muchos usuarios caen en la tentación de gastar dinero en comprar verduras para Farmville u otros complementos para juegos de la red, pero muchos resultan aburridos por el engorroso procedimiento indica el periódico El Diario (2012).

Y es que Facebook se queda con el 30% del dinero que los usuarios gastan en estas apps. Las cantidades suelen ser pequeñas, pero acaban representando hasta el 15% de los ingresos de la red social, según datos de The New York Times, de acuerdo al periódico El Diario; facebook se encuentra en plena reestructuración financiera. Sus acciones solo no han descendido desde que salieron a bolsa, y la red social necesita más dinero urgentemente. Tiene más de 900 millones de usuarios activos, pero todavía no han dado con la fórmula para rentabilizar esta cifra. El potencial de tanta gente junta es enorme, pero parece que el equipo de Mark Zuckerberg no consigue dar con la fórmula efectivizar ese gran potencial.

Los pagos se van a realizar en la moneda de cada país a través de una tarjeta de crédito. Es el sistema más sencillo, y puede ayudar a que muchos usuarios se decidan a gastar algo a través de esta red. Es el método de pago más habitual en Internet, y el que utilizan grandes compañías como Apple para su plataforma de venta de música, iTunes.

2.3.2. El Sucre

Por otra parte Bolivia y Venezuela ya implementan las monedas virtuales, quienes usan el Sucre (Sistema Unitario de Compensación Regional) como moneda única entre los países de la Alternativa Bolivariana para América y El Caribe ALBA (Alianza Bolivariana para las Américas) a diferencia del Bitcoin, el Sucre está centralizado por una autoridad máxima que en ese caso son los países que conforman el ALBA

(Venezuela, Cuba, Bolivia, Dominica, Nicaragua, San Vicente y las Granadinas, Ecuador y Uruguay), este sistema unificado de compensación Regional de Pagos, mediante un acuerdo que suscribirán ambos países, informó el ejecutivo nacional de la Micro y Pequeños Empresarios como una nueva divisa, similar al Euro, que será utilizada como medio de pago para el comercio exterior entre los miembros del ALBA

Si bien se intenta globalizar una sola moneda entre países aún no logran tener el valor único en cuanto a las divisas de diferentes países por lo que es complicado convertir el valor de una moneda de determinado país a otro valor para un diferente país.

2.4. Bitcoin

Bitcoin es una moneda electrónica descentralizada, concebida en 2009 por quien se ha dado a conocer como Satoshi Nakamoto. El nombre Bitcoin se aplica también al software libre diseñado por Nakamoto (Nakamoto, 2009) para la gestión de dicha moneda, y a la red P2P (*peer to peer,* o red de "pares" bajo un mismo protocolo) que le da soporte como una moneda ajena a controles gubernamentales o de bancos centrales.

A diferencia de la mayoría de las monedas, el funcionamiento de Bitcoin no depende de una institución central, sino de una base de datos distribuida. El software ideado por Nakamoto se vale de la criptografía para proveer funciones de seguridad básicas, tales como la garantía de que los Bitcoin sólo puedan ser gastados por su dueño, y nunca más de una vez.

El diseño de Bitcoin, de hecho, permite poseer y transferir valor entre cuentas públicas de forma potencialmente anónima. Bitcoin es una moneda completamente digital la cual está compuesta por bits generadas en la red por

Un minero digital que almacenara una cartera digital de la PC lo que vendría

Siendo la banca digital donde se es el dueño de la cartera por lo que se realizan transacciones sin terceros de confianza que en este caso es el banco quien actuó como un intermediario en las transacciones entre dos entes, además el tercero de confianza cobra un cierto monto por realizar la transacción. Además que el Bitcoin como tal es una moneda global por lo que no está centralizada por alguna autoridad gubernamental, además costos de traslado y transacción, exposición a violaciones de la seguridad y la privacidad, posibilidad de expansión crediticia con fines políticos (causa principal del ciclo económico) e inflación (pérdida del poder adquisitivo) por aumento discrecional de la masa monetaria.

Funciona en la actualidad como divisa digital aceptada por algunos comercios online -especialmente norteamericanos- y por usuarios que también la poseen para realizar transacciones en la web. Puede ser negociada en los sitios de intercambios como Mtgox.com, o por dinero real. (Infobae, 2012)

Se calcula que existen alrededor 6,5 millones de Bitcoin en circulación y según los expertos en e-commerce, podrían ser "el futuro" en transacciones digitales, reemplazando incluso al dinero real en los próximos años. Según la propia página de Bitcoin refiriendo e al tema de la seguridad, "la moneda contiene la clave pública de su propietario. Cuando esa moneda se transfiere del usuario A al usuario B, A agrega la clave pública de B a la moneda y la firma con su propia clave privada, como observamos en el Anexo 7,3. Ahora B es propietario de la moneda y puede transferirla si lo desea. Para prevenir que A pueda transferir la moneda usada a otro usuario C, una lista pública (pero anónima) de las transacciones previas se elabora por los nodos de la red Bitcoin como muestra el Anexo 7,1, y antes de cada transacción se comprueba que la moneda no haya sido transferida anteriormente" (Infobae, 2012).

Quizás el mayor logro de Satoshi Nakamoto sea el de haber resuelto el problema del doble gasto en un sistema descentralizado, que tanto ha desvelado a economistas y programadores. Para evitar que un mismo bitcoin sea gastado más de una vez por la misma persona (en otras palabras, para evitar la falsificación), la red se vale de lo que Nakamoto describe como un servidor de tiempo distribuido, que identifica y ordena secuencialmente las transacciones e impide su modificación. Esto se logra por medio de pruebas de trabajo encadenadas (las cuales se muestran como "confirmaciones"). Más adelante veremos que dicho trabajo es realizado por los ¨mineros de Bitcoin a cambio de una recompensa en Bitcoin. Si bien el envío de Bitcoin es instantáneo, y cualquier operación puede ser monitoreada en tiempo real, las confirmaciones que nos muestra la pantalla cuando usamos el software de Bitcoin vienen a representar el proceso de ¨clearing¨. A mayor número de confirmaciones, más remota será la posibilidad de ser víctima de un doble gasto. Cuando supera las cinco confirmaciones por parte de la red, una transacción es considerada técnicamente irreversible. Cabe destacar que, hasta la fecha, no se ha documentado ningún caso de doble gasto, pero es cierto que un ataque informático de este tipo es teóricamente posible, siempre y cuando el atacante controle al menos el 51% del poder computacional que protege a la red. Sin embargo, engañar a la red el tiempo suficiente como para llevar a cabo un único doble gasto implicaría una inversión tan descomunal (el poder de cómputo de la red Bitcoin es varias veces superior al de las 100 supercomputadoras más rápidas que existen, todas combinadas), y una organización tan compleja, que desde un punto de vista económico sería infinitamente más provechoso poner esos recursos a trabajar bajo las reglas del protocolo Bitcoin. (Elbitcoin, 2011)

Según los expertos, gracias a la arquitectura criptográfica de Bitcoin, una transferencia entre direcciones Bitcoin es al menos tres veces más segura que una transferencia entre cuentas bancarias (sin contar el riesgo que implica

la forzosa intromisión de terceros en el sistema bancario). Puede decirse que Bitcoin funciona como un libro contable descentralizado, en el cual los saldos no están ligados a los usuarios, sino a las direcciones públicas que ellos controlan. El historial de todos los movimientos de Bitcoin permanece almacenado en la cadena de bloques, una base de datos distribuida que mantiene el registro de todas las transacciones en cada uno de los múltiples nodos que integran la red. Estos nodos no son más que computadoras ejecutando el software de Bitcoin en todo el mundo, conectadas entre sí por medio de Internet. (Elbitcoin, 2011)

2.4.1. Historia del Bitcoin

A continuación, una breve crónica sobre el Bitcoin obtenido de (Elbitcoin, 2011):

3 de Enero de 2009: se establece el primer bloque (*Genesis block*) a las 18:15:05 hs (GMT).
11 de Enero de 2009: lanzamiento de la versión 0.1 del cliente Bitcoin.
22 de Mayo de 2010: *Laszlo* es el primer usuario en utilizar sus bitcoin para comprar una pizza. Paga BTC 10.000 (diez mil bitcoin por una pizza de US$25!).
11 de Julio de 2010: se publica en *slashdot* el lanzamiento de la versión 0.3 del cliente Bitcoin, lo cual atrae un gran flujo de nuevos usuarios.
12 de Julio de 2010: se inicia un aumento brusco (x10) del valor, que en 5 días pasa de US$0,008/BTC a US$0,08/BTC.
17 de Julio de 2010: empieza a funcionar MtGox (el primer sitio de *trading*).

6 de Noviembre de 2010: la economía de Bitcoin supera el millón de dólares. El precio en MtGox alcanza los US$0,50/BTC.

9 de Febrero de 2011: el Bitcoin alcanza la paridad con el Dólar estadounidense (1 bitcoin = 1 dólar).

14 de Febrero de 2011: se ofrece por primera vez un automóvil a cambio de bitcoin.

16 de Abril de 2011: la revista TIME publica un artículo sobre Bitcoin.

10 de Junio de 2011: el tipo de cambio hace un pico, superando los US$31, para luego caer hasta los US$10 en un lapso de cuatro días (la mayor disminución porcentual del precio hasta la fecha).

13 de Junio de 2011: el usuario del foro de Bitcoin *allinvain* anuncia que le han robado de su computadora una billetera Bitcoin con las claves privadas para acceder a BTC25.000 (veinticinco mil bitcoin, entonces equivalente a US$375.000).

19 de Junio de 2011: hackean la base de datos de MtGox y logran obtener el listado de 60.000 usuarios con sus respectivas contraseñas y direcciones de e-mail. Luego se supo que el algoritmo utilizado para proteger esa información era fácilmente vulnerable.

19 de Junio de 2011: alguien accede a una cuenta del administrador de MtGox y emite órdenes de venta por miles de Bitcoin inexistentes, forzando la caída de la cotización en MtGox desde US$17,51 hasta US$0,01 por bitcoin. MtGox luego anuncia que dichas transacciones serían revertidas, y suspende las actividades durante los siguientes 7 días.

24 de Junio de 2011: la dificultad para generar bloques supera el millón con el bloque 133056.

4 de Julio: nace ElBitcoin.org, el primer blog en español dedicado íntegramente a Bitcoin.

22 de Julio de 2011: Intervex Digital lanza BitCoin Mobile, la primera aplicación relacionada con Bitcoin para iPad.

26 de Julio de 2011: Bitomat, el tercer sitio de *trading* de bitcoins (en orden de volumen transado), sufre la pérdida de 17.000 bitcoin debido a un error técnico. (En el curso del siguiente mes, Mago adquiere Bitomat e incorpora su base de datos de usuarios; los Bitcoin pagados por MtGox en esta operación son destinados al resarcimiento de los ex-usuarios de Bitomat).

29 de Julio de 2011: MyBitcoin, el primer servicio de billetera online – el primero, el más grande y el más completo – se torna inaccesible para los usuarios. Miles de personas no pueden disponer de sus bitcoin ni saben si podrán recuperarlos. Los responsables del sitio se toman una semana para informar que la seguridad del sistema había sido vulnerada por un hacker, y luego reintegran a los usuarios sólo el 49% de sus depósitos.

19/21 de Agosto de 2011: Primera Conferencia y Exposición Mundial de Bitcoin, en Nueva York, EE.UU.

17 de Noviembre de 2011: luego de meses de lento declive, el precio del bitcoin toca fondo en US$2. Se inicia una etapa de rápida recuperación, apoyada en una nueva generación de servicios que apuntan al usuario no técnico.

25 y 26 de Noviembre de 2011: Conferencia Europea de Bitcoin y Tecnología del Futuro 2011, en Praga, República Checa. Los oradores más destacados fueron: Amir Taaki, Rick Falkvinge, Max Keiser y Stefan Thomas.

7 de Diciembre de 2011: Internet Archive, el coloso de Internet dedicado a la digitalización de todo tipo de documentos, empieza a aceptar donaciones en bitcoin. Durante los primeros dos días recibe 480 bitcoin.

27 de Diciembre de 2011: el sitio regional de Nueva York de Wikimedia (la fundación que incluye entre sus proyectos a Wikipedia) empieza a aceptar donaciones en bitcoin.

15 de Enero de 2012: Bitcoin es el tema central en un episodio de la popular serie televisiva "The Good Wife".

1 de Marzo de 2012: al menos 46.000 bitcoin son robados de "billeteras calientes" (billeteras permanentemente activas que efectúan de manera automática gran cantidad de transacciones) en un hackeo a la compañía de servicios de *hosting* Linode. El sitio de *trading* Bitcoinica y el *pool* de minería Slush – los emprendimientos más afectados por el siniestro – anuncian que continuarán funcionando con normalidad. El precio del bitcoin se mantiene sin cambios significativos (en torno a los US$5).

2 de Abril de 2012: se anuncia en el foro de Bitcoin el lanzamiento de CoinDL, el iTunes del mundo Bitcoin.

30 de Junio de 2012: YCombinator, la mayor incubadora tecnológica del mundo, anuncia que está financiando Coinbase, un servicio de cartera Bitcoin online.

23 de Julio de 2012: WIKISPEED se convierte en el primer fabricante de automóviles en aceptar Bitcoin.

Como se puede ver, su evolución fue rápida.(Anexo, [52] y [53])

2.4.2. Características de dinero Bitcoin

Estas son las características básicas de cualquier red Bitcoin:

- Bitcoin pueden ser transferidos entre nodos arbitrarios de la red.
- Las transacciones son irreversibles.
- Gasto doble se evita utilizando una cadena de bloques.

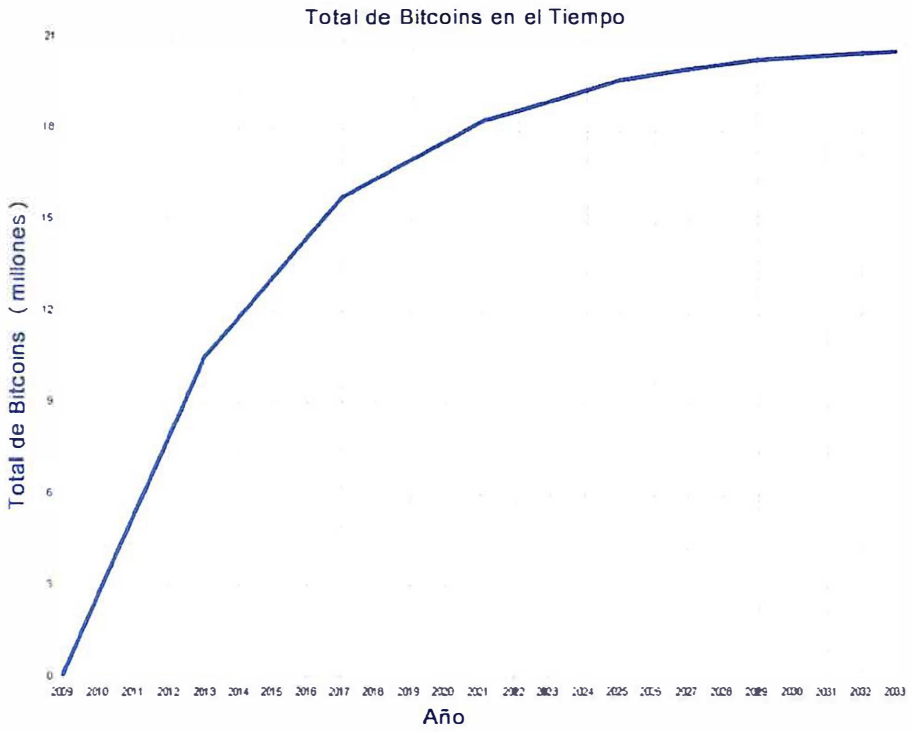
- Las transacciones se transmiten en de segundos, y verificado dentro de los 10 a 60 minutos.
- Las transacciones se pueden recibir en cualquier momento, independientemente de si el equipo está encendido o apagado.
- Mayor privacidad, al eliminar la interferencia de terceros en las transacciones.
- Aumento decreciente y predecible de la masa monetaria, lo cual ayuda a preservar – y probablemente a mejorar – el poder adquisitivo de los usuarios.
- Menores – e incluso nulos – costos de transacción en la web, cuyos niveles actuales – por ejemplo a través de PayPal – entorpecen el libre intercambio. Simplifica y acelera el pago de persona a persona, prescindiendo de intermediarios no deseados.
- Una dirección Bitcoin puede ser anónima, si así lo desea el usuario.
- Permite hacer transferencias a cualquier parte, ignorando barreras geográficas y políticas.
- Es transparente: aunque nadie está forzado a revelar su identidad, todas las transacciones quedan grabadas en un registro de libre acceso.
- Admite transacciones complejas (depósitos en custodia; seguros de depósitos; garantías; mediación, etc.) con un firme respaldo criptográfico para todo tipo de reglas y condiciones libremente acordadas por las partes.
- Nunca se detiene: no hay feriados ni fines de semana para las operaciones en Bitcoin.
- Hace viables el micro pago a gran escala.
- Impide la congelación de fondos.
- Impide la reversión involuntaria de pagos.

- Impide la restricción arbitraria de bienes y servicios que pueden adquirirse.
- Permite la acumulación de fortunas enormes en un espacio ínfimo.
- No requiere confianza en un tercero ni en un determinado sistema legal para preservar su valor.
- Facilita la protección contra el robo en todas sus formas – impuestos inclusive: la tecnología en la que se basa el protocolo de Bitcoin es varias veces más segura que la empleada por los bancos y las tarjetas de crédito.
- No puede ser eliminado ni puede falsificarse.
- Es fácil e instantáneamente reconocible. infinitamente divisible.
- Bitcoin no puede ser controlado por ninguna autoridad debido a su naturaleza descentralizada.
- La expansión de la base monetaria está predeterminada por el software de Bitcoin y es por toda conocida, de modo que no es posible afectar el poder adquisitivo de los usuarios manipulando la cantidad de Bitcoin en circulación.
- Las transferencias son realizadas directamente entre los nodos, sin un procesamiento centralizado por un tercero, lo cual hace imposible tanto la reversión involuntaria de pagos como la cancelación de transacciones mutuamente acordadas.
- El envío de Bitcoin se asemeja, en los beneficios y en los riesgos que supone, al envío de dinero en efectivo. No obstante, muchos sitios ofrecen servicios similares a e-bay o mercado libre para facilitar el intercambio de bienes y servicios por Bitcoin (por ejemplo, promoviendo la calificación entre los usuarios y/o reteniendo los fondos hasta que las partes expresan conformidad).

El software de Bitcoin (denominado "cliente Bitcoin") que los usuarios tienen instalado en sus ordenadores transmite cada transacción a los nodos cercanos, que a su vez la propagan a toda la red. Las transacciones inválidas son rechazadas por los clientes honestos (aquellos que se atienen al protocolo de la cadena de bloques en uso). Por el momento, la mayoría de las transacciones pueden realizarse gratuitamente, pero ya hemos visto que es posible pagar una tarifa para que los mineros prioricen (aceleren) su procesamiento.

El número total de Bitcoin tenderá a 21 millones con el tiempo. Su oferta crece en una serie geométrica (con una razón constante); así, en 2013 la mitad de la oferta total fue generada, y en 2017, 3/4 de la misma. A medida que la cantidad de Bitcoin se aproxime al límite de 21 millones, se espera que la economía Bitcoin entre en deflación, vale decir que el poder adquisitivo de cada bitcoin aumente, probablemente hasta alcanzar cierta estabilidad. Los Bitcoin, entre tanto, son divisibles hasta 8 decimales (dándonos 2,1 x 10 elevado a la quinceava potencia – vale decir 2,1 cuatrillones – de unidades totales), y potencialmente aún más, lo cual remueve las limitaciones prácticas a los ajustes de precio en un contexto deflacionario. (Elbitcoin, 2011)

Figura 7: Oferta de Bitcoin en el Tiempo



Fuente: El Bitcoin en español.

2.4.3. Las reglas económicas del Bitcoin

Estas reglas se aplican colectivamente por la red. Si bien no va a cambiar para Bitcoin, otras monedas digitales utilizando tecnología Bitcoin pueden cambiarlos para satisfacer sus necesidades.

- Límite duro de unos 21 millones de Bitcoin.
- Bitcoin son divisibles a 8 decimales que arrojan un total de aprox. 21×10^{14} unidades monetarias.

  Las transacciones son baratos, y sobre todo libre (gastos de transacción).

2.4.3.1 Características de la red Bitcoin

La red ha estado funcionando durante más de 45 meses cediendo a algunas características de seguridad impresionantes.

- Cadena de bloque largo (más de 204,000 bloques) con una gran cantidad de potencia de procesamiento proteger las transacciones.
- Sólo uno de los principales incidentes (fijado en agosto de 2010).

Los pagos se envían directamente de una parte a otra sin tener que pasar a través de un Institución financiera. Las firmas digitales proporcionan parte de la solución, pero el principal beneficios se pierden si un tercero de confianza sigue siendo necesario ya que lo que se quiere con el Bitcoin es evitar el doble gasto. Se propone una solución al problema de doble gasto utilizando una red peer-to-peer. Las marcas de tiempo de las transacciones de red hash ellos en una cadena continúan basado en hash de prueba de trabajo, formando un registro que no se puede cambiar sin rehacer la prueba de trabajo.

2.4.3.1.1. Comercio en internet y el Bitcoin

Comercio en Internet ha llegado a depender casi exclusivamente de las instituciones financieras que sirven como terceros de confianza para procesar los pagos electrónicos. Si bien el sistema funciona bastante bien para mayoría de las transacciones el costo de la mediación aumenta los costos de transacción, lo que limita el tamaño mínimo transacción práctico y cortando la posibilidad de que pequeñas transacciones ocasionales adema se debe tomar en cuenta cierto porcentaje de fraude ya que acepta como inevitable. Estos costes e incertidumbres de pago se pueden evitar en persona mediante el uso de moneda física, pero no existe ningún mecanismo para hacer pagos sobre un canal de comunicaciones sin una parte de confianza.

Lo que se necesita es un sistema de pago electrónico basado en la prueba criptográfica en vez de la confianza, permitiendo que cualquiera de las dos partes que desean negociar directamente entre sí sin la necesidad de un tercero de confianza. Las transacciones que son computacionalmente inviable para revertir protegerían a los vendedores de fraude y los mecanismos de compra protegerían a los compradores.

2.4.3.1.2. La red

Los pasos para ejecutar la red son los siguientes:

Las nuevas transacciones se difunden a todos los nodos, cada nodo recoge nuevas transacciones en un bloque, cada nodo trabaja en la búsqueda de una difícil prueba de trabajo de su bloque.

Cuando un nodo encuentra una prueba de trabajo, difunde el bloque a todos los nodos. Los nodos aceptan el bloque sólo si todas las transacciones en la misma red son válidas y no incurren doble gasto. Los nodos expresar su aceptación de la manzana, trabajando en la creación de la siguiente secuencia en la cadena, utilizando el hash del bloque aceptado como el hash anterior.

Los nodos siempre en cuenta la cadena más larga para ser el correcto y seguiremos trabajando en extenderlo. Si dos nodos transmiten diferentes versiones del siguiente bloque simultáneamente, algunos nodos pueden recibir uno o el otro primero. En ese caso, se trabaja en la primera recibida, sino para salvar la otra rama en caso de ser más larga. El empate se resolverá cuando la próxima prueba de trabajo se encuentra y se convierte en una rama más larga, los nodos que estaban trabajando en la otro rama entonces se cambia a la más larga las nuevas emisiones de transacción no necesariamente tienen que llegar a todos los nodos. Mientras que alcancen muchos nodos, van a entrar en una

cuadra antes de tiempo. Si un nodo no recibe un bloque, se lo pedirá cuando se recibe el siguiente bloque y de cuenta de que no se envió ni se recibió.

2.4.3.2. Cómo se generan el Bitcoin

Generar Bitcoin es conocido como "minar", lo que se refiere a la minería de metales preciosos. La probabilidad de que un usuario reciba un lote depende del poder computacional con el que contribuye a la red en relación al poder computacional de todos los otros nodos combinados. El primer nodo generador en encontrar la solución al problema criptográfico que presenta el bloque-candidato es el que obtiene un nuevo lote de Bitcoin. Los "mineros" también pueden unirse por medio de Internet para generar Bitcoin en grupo, formando un "pool minero". La cantidad de Bitcoin creada por lote nunca es ni será mayor a 50 BTC, y los premios (el número de Bitcoin por lote) están programados para disminuir con el paso del tiempo, reduciendo el incremento de la masa monetaria de manera predecible, hasta llegar a cero. Nunca llegarán a existir más de 21 millones de Bitcoin. (Elbitcoin, 2011)

Para que un bloque sea generado cada diez minutos, el protocolo actualiza cada dos semanas la dificultad del problema que todos los nodos generadores están intentando resolver, al poder computacional de toda la red. Ya que la tarea para obtener Bitcoin por medio de la minería se tornó un tanto más complica, ya hace mucho tiempo que ésta dejó de estar al alcance del usuario común de una PC. Es más sencillo obtener dinero bitcoin comprándolas en diferentes casas de cambio.

Antes de estudiar al bitcoin debemos tomar en cuenta los siguientes conceptos básicos. Por elBitcoin.org el 2 agosto, 2012 en Tutoriales

2.4.3.2.1. Red Bitcoin

Es una red de ordenadores (nodos) a través de la cual se difunden todas las transacciones Bitcoin y se mantiene *la* cadena de bloques. A veces el término también es utilizado para referirse a los mineros.

2.4.3.2.2. Hash

Es una cantidad arbitrariamente grande de datos en una longitud fija de hash, se describen generalmente como hexadecimales. Bitcoin utiliza el algoritmo SHA-2 este es un algoritmo hash para generar de manera verificable al azar, los números de una cantidad previsible de los esfuerzos de la CPU. (Bitcoin, 2012)

Por ejemplo, que te digo que he sumado dos números y que el resultado de dicha suma ha sido 14.862. Sólo con esa cifra, no hay forma de que tú sepas cuáles fueron los dos números que yo sumé. Pero sería fácil reproducir mi resultado si yo te pidiera que sumaras 3.608 y 11.254. Los hashes son mucho más complicados que esto y, aunque el resultado de una función hash parezca completamente aleatorio, proviene de operaciones matemáticas complicadas pero fáciles de reproducir.

2.4.3.2.3. SHA-2

Diseñado por la agencia de seguridad nacional (NSA) publicado el 2001 por el NIST. SHA es sinónimo de Secure Hash algorithm. SHA-2 incluye cambios significativos de su predecesor SHA-1 para la generación de contraseñas.

2.4.3.2.4. Nonce

Está en un bloque de 32 bit (4bytes) campo que se fija de modo que el valor hash del bloque contendrá ceros cualquier cambio en el Nonce hará que el Hash de bloque sea completamente diferente. (enBitcoin, 2012)

2.4.3.2.5. Cadena de bloques

Es una lista pública de todas las transacciones que se han llevado a cabo, gracias a la cual todos saben a qué clave privada pertenece cada bitcoin. Cada nodo de la Red Bitcoin contiene una copia de la cadena de bloques.

2.4.3.2.6. Bloques

Son las unidades que forman la cadena de bloques. Cada bloque contiene el hash del bloque previo (de manera que nadie pueda quitar o modificar bloques sin que esto sea detectado por la red), todas las transacciones aún no confirmadas por la red, y un número llamado nonce. Para que alguien pueda crear un bloque deberá encontrar un nonce de manera tal que el hash del bloque esté por debajo de cierto umbral (el *objetivo*). Esto sólo puede lograrse probando todos los nonces, uno tras otro, hasta que se encuentre uno con el hash deseado; cuanto menor es el objetivo, más difícil es lograrlo. El motivo por el cual la creación de bloques es deliberadamente difícil, es el de prevenir que alguien pueda gastar Bitcoin y luego crear y distribuir su propia cadena de bloques en donde no figure dicha transacción, lo cual le daría la posibilidad de gastarlos nuevamente. Cuando un bloque válido es creado, es distribuido a través de la red, y se comienza el trabajo para crear el próximo bloque. El bloque génesis es el primer bloque de la *cadena*, y fue creado el 4 de enero de 2009.

En Bitcoin, las transacciones se agrupan en trozos grandes de datos llamados bloques. Estos bloques están unidos entre sí de manera tal que cada uno prueba que el bloque anterior es válido. Cuando en tu cliente Bitcoin ves transacciones que dicen algo como "12 confirmaciones", eso significa que el bloque que contiene esa transacción se encuentra 12 bloques por detrás del actual bloque. Esto es importante, porque cuanto más "profundo" en los bloques

se encuentre una transacción, más trabajo le tomaría a un aspirante de hacker retroceder en el tiempo y efectuar algún cambio.

2.4.3.2.7. Transacción sin confirmar

Una es aquella que aún no forma parte de un bloque.

2.4.3.2.8. Confirmación

Ocurre cuando una transacción es incluida en un bloque para formar parte de la cadena de bloques de forma permanente.

2.4.3.2.9. Confirmaciones

Significa que la transacción pertenece a un bloque y que hay 5 bloques posteriores a éste en la cadena; lo cual provee una mayor seguridad de que dicha transacción es legítima.

2.4.3.2.10. Minero

Es alguien que intenta crear bloques para agregar a la *cadena* (el término también puede referirse al software dedicado a tal fin). Los mineros son recompensados por su trabajo por el protocolo Bitcoin, que automáticamente asigna 50 nuevos Bitcoin al minero que cree un bloque válido. Ésta es la forma en la que se crea el Bitcoin. Cada 4 años, el premio por bloque disminuye a la mitad.

2.4.3.2.11. Dificultad

Indica qué tan complicado es crear un nuevo bloque (la inversa del objetivo), y se ajusta automáticamente para asegurar que a la red le tome un promedio de 10 minutos el encontrar un bloque válido.

2.4.3.2.12. Ataque del 51%

Es un intento de obtener el poder de bloquear y revertir transacciones Bitcoin a través de la obtención y el uso de un pool computacional lo suficientemente poderoso como para dominar al resto de la *red Bitcoin* (controlando al menos el 51% de la misma).

2.4.3.2.13. Doble gasto

Es un intento de enviar los mismos Bitcoin dos veces. Los mineros previenen que esto suceda, pero tal ataque es posible contra usuarios que aceptan transacciones sin confirmar y en conjunto con un ataque del 51%.

(Bitcoinmagazine, 2012)

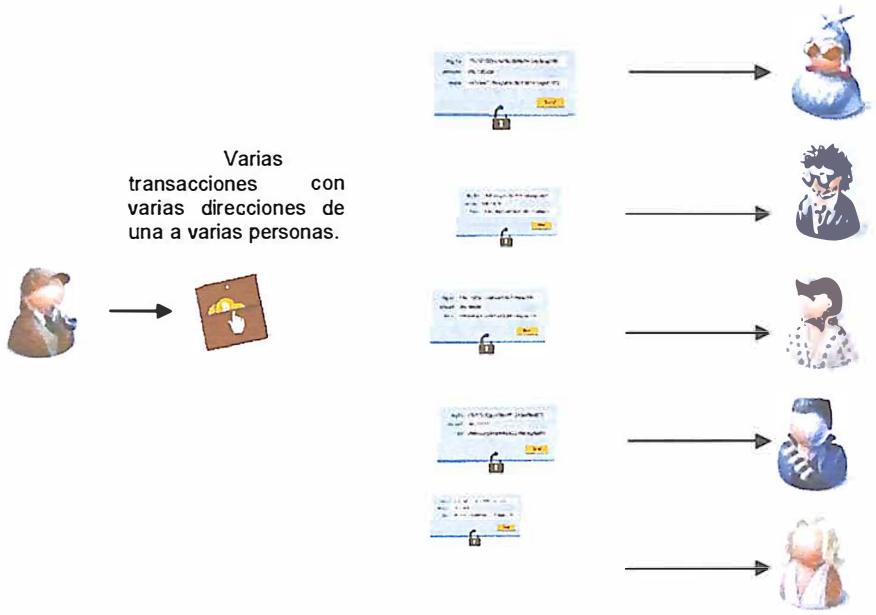
2.4.3.3. Cuenta Bitcoin (BTC)

Cualquier persona que participa en la red Bitcoin posee una billetera electrónica que contiene pares de llaves criptográficas. Las direcciones Bitcoin visibles derivan de las llaves públicas del usuario, y funcionan como los puntos remitente *o* receptor para todos los pagos. Las llaves privadas correspondientes a cada llave pública sirven para que un determinado usuario autorice pagos (transfiera Bitcoin) desde su billetera.

Las direcciones públicas no tienen ninguna información sobre sus dueños; éstas aparecen como secuencias aleatorias de números y letras de 33 caracteres de largo, como por ejemplo: 1rYK1YzEGa59pl314159KUF2Za4jAYYTd. Los usuarios de Bitcoin pueden tener múltiples direcciones; de hecho, pueden generar direcciones nuevas fácilmente y sin límites. Generar una nueva dirección equivale a generar un nuevo par de llaves (pública/privada), y no requiere ningún contacto con nodos

de la red. Los usuarios que desean preservar el anonimato suelen crear una nueva dirección para cada transacción.

Figura 8: Usuarios de Bitcoin con múltiples direcciones en las transacciones.



Fuente: Elaboración propia.

2.4.3.4. Transacciones

Cuando un usuario Rene transfiere Bitcoin a Gaby, Rene renuncia a su posesión de un determinado número de Bitcoin, agregándoles la llave pública de Gaby y firmando la combinación resultante con su llave privada. (Gracias al empleo de la criptografía asimétrica, la llave privada no puede ser deducida de la firma que de ella deriva). Esta información se transmite a toda la red P2P como una nueva transacción. Entonces, el resto de los nodos de la red verifican

el número de Bitcoin involucrados y la autenticidad de las firmas criptográficas, antes de aceptar la transacción como válida.

Para nuestros propósitos, la transacción más antigua es la que cuenta, así que no me importa sobre los intentos posteriores de doble gastar. La única forma de confirmar la ausencia de una transacción es estar al tanto de todas las transacciones.

La fecha y hora del servidor nos permitirá sabes el origen de un Hash lo que un servidor de marca de tiempo consiste en tomar una hash de un bloque de elementos que se fechados y publicar ampliamente el hash, tal como en un periódico. La marca de tiempo demuestra que los datos deben haber existido en el entonces, obviamente, con el fin de entrar en el hash. Cada marca de tiempo incluye la marca de tiempo anterior en su hash, formando una cadena, con cada marca de tiempo adicional de refuerzo los que conoce.

2.4.3.4.1. La prueba de trabajo

La prueba de trabajo implica la exploración de un valor que cuando se aplica un algoritmo hash, tal como con SHA-256, el Hash comienza con un número de bits a cero. El promedio de trabajo necesario es exponencial en el número de cero bits requerida y puede ser verificada mediante la ejecución de un hash único.

Para nuestra red de fecha y hora, ponemos en práctica la prueba de trabajo incrementando un nonce en el bloque hasta que encuentra un valor que le da al bloque de hash de los requeridos cero bits. Una vez que la CPU se ha dedicado a hacer cumplir la prueba de trabajo, el bloque no se puede cambiar sin rehacer el trabajo. Como los bloques posteriores se encadenan después de él, el trabajo de cambiar el bloque incluiría a rehacer todos los bloques después de él.

La mayoría decisión está representada por la cadena más larga, que tiene la mayor prueba de esfuerzo de trabajo invertido en ella. Si la mayoría de energía de la CPU está controlada por los nodos honestos, la cadena honesta crecerá el más rápido y superará cualquier cadena competidoras. Para modificar una cuadra después, un atacante tendría que hacer de nuevo la prueba de trabajo del bloque y después todos los bloques y luego alcanzar y superar el trabajo de los nodos honestos. Veremos más adelante que la probabilidad de que un atacante más lento alcanzando disminuye exponencialmente a medida que los bloques subsiguientes se añaden.

Para compensar la creciente velocidad del hardware y el interés que varían en marcha los nodos con el tiempo, la dificultad de prueba de trabajo está determinada por un promedio móvil de focalización un número medio de bloques por hora. Si están generado demasiado rápido, la dificultad aumenta.

2.4.3.4.2. Espacio en disco

Una vez que la última transacción en una moneda está enterrada bajo suficientes bloques, las transacciones pasaron antes que puede ser descartada para ahorrar espacio en disco. Para facilitar esto sin romper el hash del bloque, operaciones son ordenadas en un árbol Merkle, sólo la raíz incluida en el hash del bloque. Viejos bloques entonces se puede compactar por stubbing las ramas del árbol. Los hashes interiores hacer no necesitan ser almacenados.

Un encabezado de bloque con ninguna transacción sería de unos 80 bytes. Si suponemos que los bloques se generan cada 10 minutos, 80 bytes * 6 * 24 * 365 = 4.2MB por año. Con los sistemas informáticos típicamente vende con 2 GB de RAM a partir de 2008, y la Ley de Moore predecir el crecimiento actual de 1,2 GB por año, el almacenamiento no debería ser un problema

incluso si las cabeceras de bloque se debe mantener en memoria. Como podemos observar en el Anexo 7,3.

2.4.3.4.3. Pago y verificación

Es posible verificar los pagos sin ejecutar un nodo de red completa. Un usuario sólo necesita mantener una copia de los encabezados de bloque de los más largos de prueba de trabajo de la cadena, la cual puede obtener mediante la consulta los nodos de la red hasta que se haya convencido de que tiene la cadena más larga, y obtener la rama Merkle vincular la operación en el bloque de marca de tiempo él no puede comprobar la transacción para sí mismo, sino por su vinculación a un lugar en la cadena, se puede ver que un nodo de red ha aceptado, y los bloques añadidos después de que se confirman aún más la red ha aceptado cabe señalar que cuando una operación depende de varias transacciones, y las transacciones dependen de muchos más, no es un problema aquí. No hay nunca la necesidad de extraer una completa copia independiente de la historia de una transacción como un servidor de seguridad adicional, un nuevo par de claves debe ser usado para cada transacción para evitar de estar vinculado a un propietario común. Si no se cambian de manera constante las cuentas de usuario en las billeteras es inevitable que con múltiples entradas en las transacciones, necesariamente revelan que sus entradas eran propiedad del mismo dueño. El riesgo es que si el propietario de una clave se revela, vinculando podría revelar otras transacciones que pertenecían a el mismo propietario.

2.4.3.4.4. Cálculos

Consideramos que el escenario de un atacante tratando de generar una cadena alternativa más rápida que la cadena honesta. Incluso si esto se logra,

no lanzar el sistema abierto a cambios arbitrarios, tales como la creación de valor a partir de la nada o tomar dinero nunca que pertenecía al atacante. No vamos a aceptar una transacción no válida como forma de pago, y los nodos honestos nunca aceptará un bloque que los contiene. Un atacante sólo puede tratar de cambiar a uno de sus propias operaciones para recuperar dinero que hace poco se ha gastado.

La carrera entre la cadena y una cadena honesto atacante puede ser caracterizado como un binomio Random. El evento de éxito es la cadena honesto que se prorrogó un bloque, incrementando su conducir por 1, y el evento falla es la cadena del atacante está extendiendo por una cuadra, lo que reduce la brecha por -1.

La probabilidad de que un atacante se ponga al día de un déficit dado es análogo al de un Gambler Ruina problema. Supongamos que un jugador con crédito ilimitado comienza en un déficit y juega potencialmente un número infinito de ensayos para tratar de alcanzar el punto de equilibrio. Podemos calcular la probabilidad de que alguna vez alcanza el punto de equilibrio, o que un atacante siempre se pone al día con la cadena de honesto, de la siguiente manera:

p = probabilidad de que un nodo honesto encuentra el siguiente bloque

q = probabilidad de que el atacante se encuentra el siguiente bloque

z = Probabilidad de que el atacante nunca se pondrá al día a partir de bloques z detrás

Dada nuestra hipótesis de que $p > q$, la probabilidad disminuye exponencialmente a medida que el número de bloques de los atacante tiene que ponerse al día con los aumentos. Con las probabilidades en su contra, si no hace una suerte de estocada hacia delante desde el principio, sus posibilidades de llegar a ser infinitamente pequeño a medida que cae más atrás.

Consideremos ahora el tiempo que el destinatario de una nueva transacción necesita esperar antes de ser suficientemente seguro de que el remitente no puede cambiar la transacción. Asumimos que el remitente es un atacante que quiere hacer creer que el destinatario le pagó por un tiempo, luego cambie a pagar a sí mismo después de algún tiempo ha pasado. El receptor recibirá una alerta cuando esto sucede, pero el remitente espera que sea demasiado tarde.

El receptor genera un nuevo par de claves y da la clave pública al remitente poco antes la firma. Esto impide que el remitente de la preparación de una cadena de bloques antes de tiempo al trabajar en de forma continua hasta que se tiene la suerte de conseguir lo suficiente por delante, a continuación, ejecutar la transacción ese momento. Una vez que la transacción sea enviada, el remitente deshonesto comienza a trabajar en secreto en una cadena paralelo que contiene una versión alternativa de su transacción.

El receptor espera hasta que la transacción ha sido añadida a un bloque y los bloques han sido *z* vinculada después de ella. No sabe la cantidad exacta de los progresos que el atacante ha hecho, pero asumiendo los bloques honestos se tomó el tiempo medio previsto por bloque, el potencial del atacante progreso será una distribución de Poisson con valor esperado. Para obtener la probabilidad de que el atacante podría tomar hasta ahora, se multiplica la densidad de Poisson para cada cantidad de progreso que podría haber hecho por la probabilidad de que podía ponerse al día a partir de ese punto. Como podemos observar en la figura.

Figura 9: Distribución de Poisson - La conversión a código C.

```
# Include <math.h>
AttackerSuccessProbability doble (doble q, int z)
{
        doble p = 1,0 - q;
        doble lambda = z * (q / p);
        doble suma = 1,0;
        int i, k;
        para (k = 0, k <= z; k + +)
        {
        doble poisson = exp (-lambda);
                for (i = 1; i <= k, i + +)
                        poisson * = lambda / i;
                        suma - = poisson * (1 - pow (q / p, z - k));
        }
        volver suma;
}
```

Fuente: El Bitcoin en español

Ejecución de algunos resultados, podemos ver que la probabilidad dejar exponencialmente con z.

q = 0,1

z = 0 P = 1,0000000

z = 1 P = 0,2045873

z = 2 P = 0,0509779

z = 3 P = 0,0131722

z = 4 P = 0,0034552

z = 5 P = 0,0009137

z = 6 P = 0,0002428

z = 7 p = 0,0000647

z = 8 P = 0,0000173

z = 9 P = 0,0000046

z = 10 P = 0,0000012

q = 0,3

z = 0 P = 1,0000000

z = 5 P = 0,1773523

z = 10 P = 0,0416605

z = 15 P = 0,0101008

z = 20 P = 0,0024804

z = 25 P = 0,0006132

z = 30 P = 0,0001522

z = 35 P = 0,0000379

z = 40 P = 0,0000095

z = 45 P = 0,0000024

z = 50 P = 0,0000006

Resolviendo para P menor que 0,1% ...

P <0,001

q = 0,10 z = 5

q = 0,15 z = 8

q = 0,20 z = 11

q = 0,25 z = 15

q = 0,30 z = 24

q = 0,35 z = 41

q = 0,40 z = 89

q = 0,45 z = 340

Lo que nos muestra que tanto PQ y Z; siempre serán en un 100% menor a un 10%

2.4.3.5. Tarifa de una transacción

La comisión de una transacción es voluntaria pero al hacerlo, además de acelerar la transacción proveen incentivos a los usuarios que mantienen nodos generadores (vale decir, a los mineros). Por ejemplo, si decidimos enviar 100 Bitcoin puede que el software nos sugiera pagar una tarifa de 0,005 Bitcoin. Las tarifas de transacción irán cobrando más importancia cuanto más bajo sea el premio por bloque. En el futuro, los mineros se verán motivados a mantener los nodos generadores por la suma de pagos en concepto de tarifas que puedan acumular, más que por los Bitcoin que sean capaces de generar.

2.4.3.6. Cadena de bloques

Cualquier transacción transmitida a otros nodos no se convierte inmediatamente en "oficial"; primero debe ser confirmada en una lista –mantenida colectivamente –de todas las transacciones conocidas: la cadena de bloques. Tal es el trabajo de los 11nodos generadores", cuyos dueños son los "mineros de Bitcoin".

Cada nodo generador de Bitcoin recoge todas las transacciones que aún no fueron confirmadas en un archivo (el bloque candidato) que contiene la referencia a dichas transacciones y al último bloque válido conocido por ese nodo. Entonces, los nodos generadores compiten entre sí tratando de encontrar un hash de ese bloque (un código aleatorio que lo representa), en un esfuerzo computacional que demanda cantidades predecibles de intento y error. Cuando un nodo encuentra la solución, la transmite a toda la red. El resto de los nodos reciben el nuevo bloque solucionado, lo verifican antes de aceptarlo y lo agregan a la cadena. Aunque ningún usuario de Bitcoin está forzado a revelar su identidad, todas las transacciones jamás realizadas quedan grabadas en esa base de datos de libre acceso que es la cadena de bloques. Esta contiene el historial de posesión de todas las monedas (o fracciones de monedas), desde la dirección creadora hasta la dirección del actual dueño, y se encuentra en todas las computadoras que ejecutan el software de Bitcoin. Por lo tanto, si un usuario intenta reutilizar monedas que él mismo ya gastó (doble gasto), la red lo detectará y rechazará la transacción. (Elbitcoin, 2011)

2.5. Moneda P2P

La naturaleza P2P de la red Bitcoin hace imposible el establecimiento de un control centralizado de todo el sistema. Esto impide el aumento arbitrario de la cantidad de Bitcoin en circulación (lo que generaría inflación) y cualquier otro tipo de manipulación del valor por parte de las autoridades.

Bitcoin es una de las primeras implementaciones de un concepto llamado cripta - moneda, que fue descrita por primera vez en | 998 por Dai Wei en la lista de correo cypherpunks. Basándose en la idea de que el dinero es un objeto, o cualquier tipo de registro, aceptado como pago de bienes y servicios y el pago de las deudas en un determinado país o contexto socio-económico, Bitcoin se ha diseñado en torno a la idea de utilizar la criptografía para controlar la creación y la transferencia de dinero, en lugar de depender de las autoridades centrales.

2.6. Ingeniería de software

Ingeniería de software es la disciplina o área de la informática que ofrece métodos y técnicas para desarrollar y mantener software de calidad. (Pressman, 2002)

Dado el propósito del presente proyecto, se describirá a la Ingeniería de Software desde el punto de vista del producto, que representa el móvil, y del proceso, la metodología por la cual pasa el software para llegar a ser producto.

2.6.1. Rational Process Unified (RUP) de IBM

Las técnicas del desarrollo del software han ido evolucionando conforme van pasando los años con el objetivo de garantizar la calidad del producto y estimular la eficiencia en el que se desarrolla estos, apareciendo paradigmas y metodologías variados desde el modelo cascada, pasando por el modelo orientado a objetos y forjándose a otros más sofisticados.

Al final de la pasada década, Grady Booch, James Rumbaugh e Ivar Jacobson empezaron a colaborar para combinar y recopilar las mejores características de cada uno de sus métodos de diseño y análisis orientado a objetos en un método unificado. El resultado, denominado *lenguaje de modelado unificado (UML),* se ha convertido en el método más utilizado por la industria. (Pressman, 2002)

RUP es un producto de IBM que se caracteriza por ser un proceso de ingenieria de software bien definido y estructurado, que engloba muchas practicas y tecnicas modernas en el desarrollo de software que es facilmente aplicable a varios organizaciones y proyectos.

Un conjunto de actividades y tareas transformaran los requerimientos de nuestro proyecto en un isstema de software. Lo que el RUP hace es asignar etas responsabilidades con la idea de producir software de alta calidad que satisfaga las necesidades de los clientes, según el tiempo y presupuesto displonible.

2.6.1.1. Características del RUP

Los creadores de esta metodología definen al RUP como "Un proceso de desarrollo de software; esto es un conjunto de actividades necesarias para

transformar los requisitos de un usuario en un sistema de software". (Jacobson, 2000)

La herramienta que usa el lenguaje de modelado unificado (UML) para poder crear todos lo esquemas que componen este metodo. Escencialmente se rigen por tres pilares relebantes:

- ✓ Es dirigido por casos de uso.
- ✓ Esta centrado en la arquitectura.
- ✓ Es iterativo e incremental.

2.6.1.1.1. Guiado por casos de uso

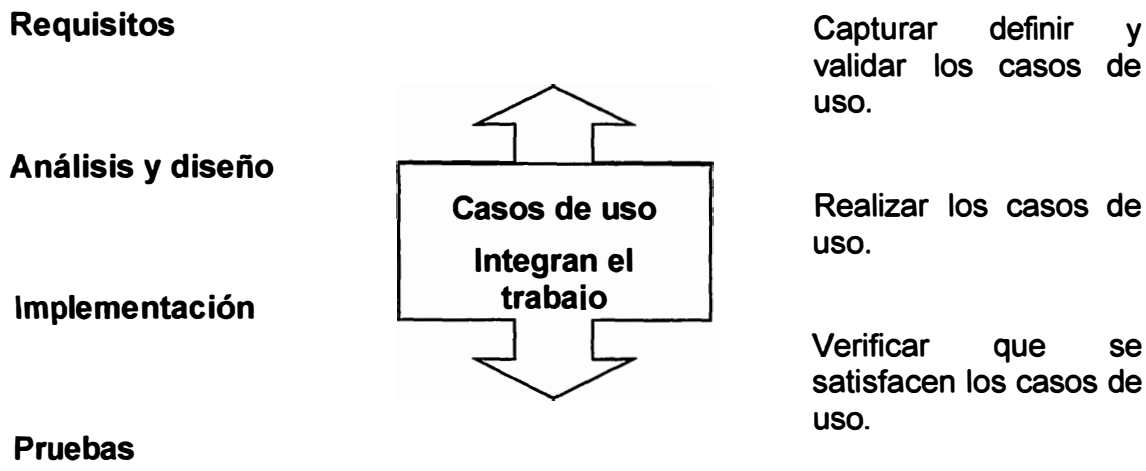
Para poder conocer y entender lo que los futuros usuarios necesitan y desean se realizan los casos de uso, estos son interacciones entre el sistema y el usuario.

"un caso de uso es un fragmento de funcionalidad del sistema que proporciona al usuario un resultado importante. Los casos de uso representan los requisitos funcionales." (Jacobson, 2000) por eso estos elementos remplazan anteriores formas de especificar las funciones de un sistema y se convierten en una guía fundamental para la realización de actividades para el proceso de desarrollo.

Los casos de uso resultan una guía a lo largo de todas las actividades desempeñadas en los flujos de trabajo, resultan importantes al momento de diseñar, desarrollar e implementar porque describen exactamente el producto final.

Las fases del RUP que conforman el siclo de vida de nuestro sistema son: Inicio, elaboración, construcción y transición, estas a su vez se dividen en iteraciones.

Figura 10: Los casos de uso a lo largo del proyecto



Fuente: Introducción de Rational Process RUP, Patricio Letelier [199-].

2.6.1.1.2. Centrado en la arquitectura

El concepto de la arquitectura del software se enfoca en los aspectos estáticos y dinámicos más relevantes del sistema. Se refiere a la relación directa de la creación del software y los medios externos que le influencian. Los más comunes son plataformas de software, sistemas operativos, bases de datos, protocolos y otros sistemas. La arquitectura debe permitir el desarrollo de todos los casos de uso requeridos, donde debe tomar en consideración elementos de calidad del sistema, rendimiento, realización y capacidad de evolución por lo que deberá ser flexible a lo largo del proyecto.

2.6.1.1.3. Iterativo e incremental

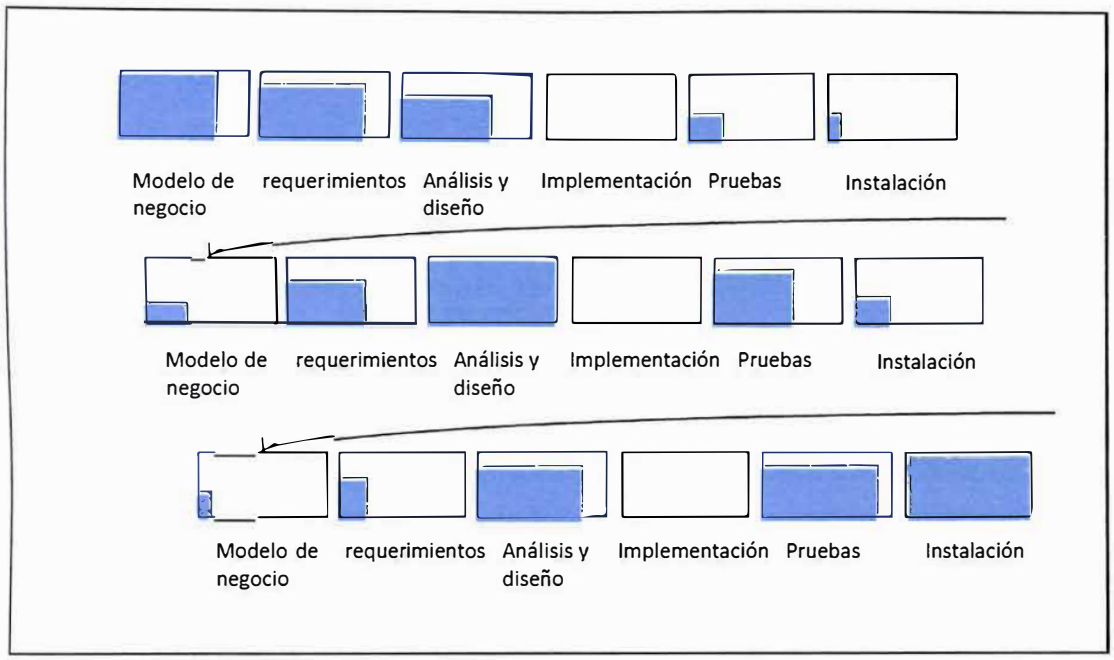
Los cambios son inevitables en todos los proyectos de software, los requerimientos del usuario van cambiando a medida q la tecnología va mejorando. Mientras vayamos encontrando variaciones a lo largo del camino debemos reorganizar las actividades de nuestro siclo de vida del sistema.

El proyecto se debe dividir en ciclos y para cada ciclo existen fases, cada una de las cuales se deberá considerar como un mini proyecto cuyo proceso sigue las iteraciones necesarias de los flujos de trabajo.

Cada iteración comprende:

- ✓ Planificar la iteración (estudio de riesgos).
- ✓ Análisis de los Casos de Uso y escenarios.
- ✓ Diseño de opciones arquitectónicas.
- ✓ Codificación y pruebas. La integración del nuevo código con el existente de las iteraciones anteriores se hace gradualmente durante la construcción.
- ✓ Evaluación de la entrega ejecutable (evaluación del prototipo en función de las pruebas y de los criterios definidos).
- ✓ Preparación de la entrega (documentación e instalación del prototipo).

Figura 11: El proceso iterativo de RUP

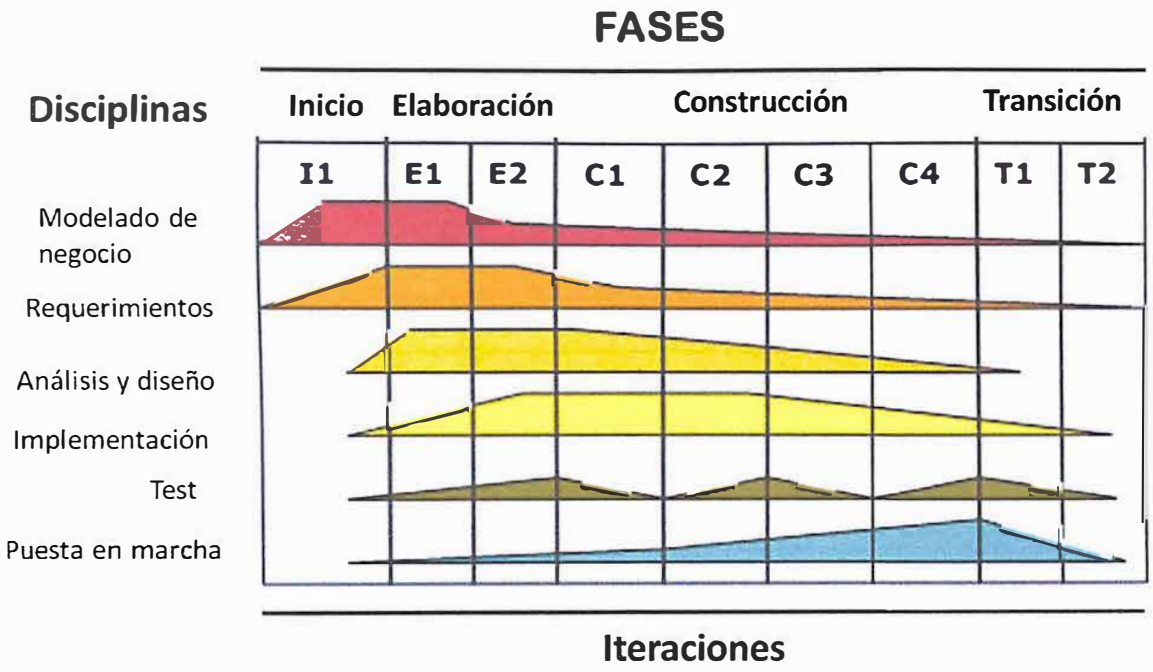


Fuente: Introducción a Rational Process (RUP), Patricio Letelier [199-]

2.6.1.1.4. Arquitectura del RUP

El ciclo de desarrollo a lo largo del tiempo, dentro de cada fase el desarrollador podrá dividir en iteraciones según la necesidad. Cada fase termina con hito, que es un entregable definido según la planificación realizada en el inicio. Cada hito es crucial para poder iniciar la siguiente fase, es obligación de los gestores del proyecto revisar y controlar que se están cumpliendo a cabalidad las fases y los entregables cumplen los objetivos.

Figura 12: Fases y flujos de trabajo del RUP



Fuente: El proceso unificado de software, Jacobson, Booch & Rumbaugh, 2000.Pag.11

Se debe recordar que cada fase se divide normalmente en iteraciones y cada iteración pasa por todas las disciplinas descritas en la Figura 8, a continuación vemos los hitos por cada fase y si son necesarias una o varias iteraciones.

Tabla 2: Hitos por cada fase

Descripción	Hito
Fase de inicio	En esta fase se obtendrán los requerimientos del producto de parte del usuario, recopilados a una lista de necesidades del área micro empresarial los principales casos de uso serán diseñados para hacer un refinamiento del plan de desarrollo del proyecto.
Fase de elaboración	Analizaremos todos los requisitos en el análisis y diseño. El diseño en diagramas UML del sistema que marca el final de esta fase.
Fase de construcción	En esta fase terminamos de analizar y diseñar los casos de uso. El producto se construye a en base a varias iteraciones, cada una produciendo un prototipo a la que se le aplican las pruebas, el hito que da fin a esta fase es la versión del prototipo con la capacidad operacional del producto lista para hacer pruebas beta.
Fase de transición	En esta fase se preparara el prototipo final, el hito final de esta fase incluye la entrega de toda la documentación del proyecto con los manuales de instalación y el software a la microempresa.

Fuente: Tabla obtenida de acuerdo a la definición de fases y flujos del modelo RUP

2.6.2. Lenguaje unificado de modelado (UML)

El Lenguaje Unificado de Modelado es un lenguaje de modelado visual que se usa para especificar, visualizar, construir y documentar artefactos de un sistema de software. Captura decisiones y conocimiento sobre los sistemas que se deben construir. Se usa para entender, diseñar, configurar, mantener y controlar la información sobre tales sistemas. Está pensado para usarse con todos los métodos de desarrollo, etapas del ciclo de vida, dominios de aplicación y medios. UML incluye conceptos semánticos, notación y principios generales. Tiene partes estáticas, dinámicas, de entorno y organizativas. (Jacobson, 2000)

UML tiene una representación en diagramas, los cuales se categorizan en diagramas de estructura, diagramas de comportamiento, diagramas de interacción.

En los diagramas de estructura se tiene:

2.6.2.1. Diagramas de Casos de Uso

Describe comportamiento del sistema al afrontar una tarea de negocio o un requisito de negocio. Esta descripción se enfoca en el valor suministrado por el sistema a entidades externas tales como usuarios humanos u otros sistemas.

2.6.2.2. Diagrama de secuencia

La interacción entre actores, las interfaces y las bases de datos la realizan los mensajes que es envían entre ellos. Se representan mediante el diagrama de secuencias que también muestra el tiempo.

Se hace un diagrama de secuencias por cada escenario para razonar más en detalle como es el comportamiento de un escenario y obtener nuevas clases y objetos en el escenario.

Se utilizan en las fases de prueba para validar el código en detalle y los tipos de datos que se envían en cada secuencia.

2.6.2.3. Diagramas de clases

Es un tipo de diagrama estático que describe la estructura de un sistema mostrando sus clases, atributos y las relaciones entre ellos. Los diagramas de clases son utilizados durante el proceso de análisis y diseño de los sistemas, donde se crea el diseño conceptual de la información que se manejará en el sistema, y los componentes que se encargaran del funcionamiento y la relación entre uno y otro.

2.6.2.4. Diagrama de componentes

Representa cómo un sistema de software es dividido en componentes y muestra las dependencias entre estos componentes. Los componentes físicos incluyen archivos, cabeceras, bibliotecas compartidas, módulos, ejecutables, o paquetes. Los diagramas de Componentes prevalecen en el campo de la arquitectura de software pero pueden ser usados para modelar y documentar cualquier arquitectura de sistema.

2.6.3. Conceptos de la arquitectura del prototipo

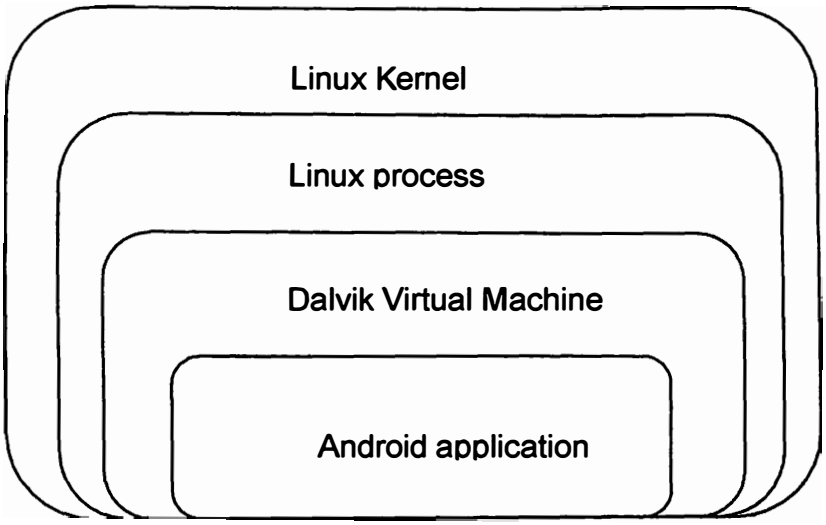
2.6.3.1. Android

Android es un sistema operativo para dispositivos móviles (celulares, Tablet, etc.) desarrollado principalmente por Google. Android sigue la filosofía de código abierto, por lo tanto, cualquier persona puede bajar el código, modificarlo dependiendo sus necesidades, y compartir esas modificaciones con la comunidad. (Triana, 2011)

2.6.3.1.1. Arquitectura de Android

Como mencionamos, Android se ejecuta encima del kernel Linux. Las aplicaciones Android se encuentran escritas en el lenguaje de programación Java y se ejecutan dentro de una máquina digital (VM). Es importante tener en cuenta que la VM no es una JVM como se podría esperar, pero es la Dalvik Virtual Machine, una tecnología de código abierto. Cada aplicación Android se ejecuta dentro de una instancia de la Dalvik VM, que a su vez permanece dentro de un proceso gestionado por el kernel Linux, como se muestra a continuación. (Ableson, 2013)

Figura 13: Dalvik VM



Fuente: Dalvik VM Ableson

Una aplicación Android que consiste en una o más de las siguientes clasificaciones:

Actividades

Una aplicación que tiene una UI visible se implementa con una actividad. Cuando un usuario selecciona una aplicación desde la pantalla de inicio o el iniciador de aplicación, se inicia una actividad.

Servicios

Se debería usar un servicio para cualquier aplicación que necesite persistir por mucho tiempo, como por ejemplo un supervisor de red o una aplicación de comprobación de actualización.

Proveedores de contenido

Es posible considerar los proveedores de contenido como un servidor de base de datos. El trabajo de un proveedor de contenido es gestionar el acceso a los datos persistentes, como por ejemplo una base de datos SQLite. Si su aplicación es muy simple, usted no debe crear necesariamente un proveedor de contenido. Si está desarrollando una aplicación más grande o una que ponga a disposición los datos para múltiples actividades o aplicaciones, un proveedor de contenido es el medio para acceder a sus datos.

Receptores de difusión

Se puede lanzar una aplicación Android para procesar un elemento de datos o para responder a un evento, como por ejemplo la recepción de un mensaje de texto.

Una aplicación Android, junto con un archivo llamado AndroidManifest.xml, se despliega para un dispositivo. AndroidManifest.xml contiene la información de configuración necesaria para instalarlo adecuadamente en el dispositivo. Incluye los nombres de clases requeridos y los tipos de eventos que la aplicación puede procesar y los permisos requeridos que la aplicación necesita para ejecutarse. A modo de Figura, si una aplicación requiere de acceso a la red — para descargar un archivo, por ejemplo — este permiso debe estar mencionado explícitamente en el archivo manifiesto. Muchas aplicaciones pueden tener este permiso específico habilitado. Tal seguridad declarativa ayuda a reducir las probabilidades de que una aplicación maliciosa pueda causar daño en su dispositivo.

La siguiente sección discute el entorno de desarrollo necesario para desarrollar una aplicación Android. (Ableson, 2013)

2.6.3.1.2.Plataforma de Android

Con la amplitud de las capacidades de Android, sería fácil confundirlo con un sistema operativo de computadora de escritorio. Androides un entorno en capas que usa de base el kernel Linux e incluye vastas funciones. El subsistema de la UI incluye:

- Windows
- Vistas
- Widgets para mostrar los elementos comunes como los recuadros para editar, las listas y las listas desplegables.

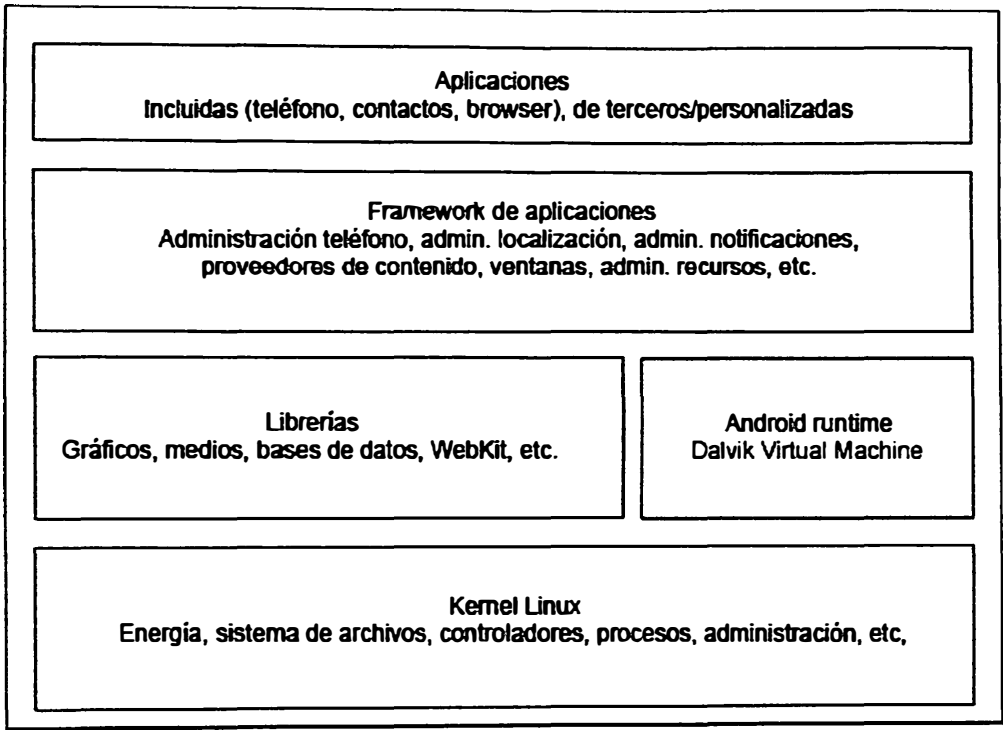
Android incluye un navegador integrable basado en WebKit, el mismo motor de navegador de código abierto que alimenta el navegador Mobile Safari de iPhone.

Android cuenta con una abundante variedad de opciones de conectividad, que incluyen Wi-Fi, Bluetooth y datos inalámbricos sobre una conexión de celular (por ejemplo, GPRS, EDGE y 3G). Una técnica popular en las aplicaciones Android es unirse a Google Maps para mostrar una dirección directamente dentro de una aplicación. El soporte para los servicios basados en la ubicación (como por ejemplo el GPS) y los acelerómetros está disponible también en la pila de software de Android. También existe un soporte para cámara.

Históricamente, las dos áreas en las que las aplicaciones móviles se han esforzado para mantenerse al día con sus homólogos de escritorio son las de gráficos/soporte físico y métodos de almacenamiento de datos. Android trata el desafío de los gráficos con soporte incorporado para gráficos en 2D y 3D, incluida la biblioteca OpenGL. La carga de almacenamiento de datos se facilita porque la plataforma Android incluye la conocida base de datos de código

abierto SQLite. La Figura 1 0 muestra una vista simplificada de las capas del software para Android. (Ableson, 2013)

Figura 14. Capas del software para Android



Fuente: Tomado de Dalvik VM Ableson [199-]

2.6.3.2. HTML 5.0

HTML es el acrónimo en inglés de HyperText Markup Language (en español se traduce como lenguaje de marcado de hipertexto). HTML 5 es el nombre que se usa para referirse a la quinta revisión del lenguaje HTML. Una característica especial de HTML 5 es que es el resultado de agrupar las especificaciones relacionadas al desarrollo de páginas web: HTML 4 (es el estándar en uso desde 1997), XHTML 1 (enlace en inglés), DOM nivel 2

(Document Object Model -Modelo de objetos del documento, en español-), e integrar algunos elementos de CSSnivel 2.

Las principales diferencias entre HTLM 5 y HTML 4 se pueden agrupar en cuatro grandes grupos:

- **Sintaxis**.-La sintaxis de HTML 5 es compatible con HTML 4 y XHTML 1. Con HTML 5 se puede usar sintaxis de XML. Con HTML 5 se puede usar sintaxis de MathML, que es un lenguaje usando para describir notaciones matemáticas, permitiendo la integración de fórmulas matemáticas a Internet.

- **Nuevos elementos y nuevos atributos**.-Además de agregar elementos nuevos al lenguaje, a algunos elementos existentes se le agregan atributos, y otros elementos cambian. Para información detallada de estas diferencias, puedes consultar la página oficial de WC3 que describe las diferencias en lenguaje entre HTML 4 y HTML 5.

- Modelo del contenido.-HTML 5 busca reducir la confusión en el concepto de bloques existente entre HTML 4 y CSS. Con este fin, define nuevas categorías y define qué elementos son parte de cada una. Para mayor información, puedes consultar la sección de cambios al modelo del contenido, descrito en la página oficial de WC3.

- APIs.-HTML5 agregó nuevas APIs (un API son las siglas en inglés de Application Programming Interface, que es una biblioteca de utilerías que puede ser utilizada por algún software, en este caso aplicaciones de Internet), además de que extendió, cambió o hizo obsoletas algunas de las ya existentes. HTML 5, hasta septiembre del 2012, aún no se ha terminado de desarrollar la fecha que tiene anunciada WC3 para terminar la especificación es el 2014),

aunque eso no significa que no se esté utilizando ya. En el medio de desarrollo de aplicaciones web se menciona a HTML 5 como la tecnología que permitirá reemplazar a Adobe Flash, dada su capacidad para integrar elementos multimedia. Opera fue quien propuso este estándar originalmente, y es uno de los principales promotores de esta tecnología, junto con Mozilla Foundation, estos últimos siendo los creadores del navegador Firefox. (Castro, 20|3)

2.6.3.3. Jquery Movile & PhoneGap

Para poder combinar con éxito jQuery Mobile con PhoneGap, debemos antes saber acerca de ellos. El marco móvil de jQuery toma el "escribir menos, hacer más". En lugar de escribir aplicaciones únicas para cada dispositivo móvil o sistema operativo, el marco móvil jQuery le permite diseñar un sitio web altamente calificado-o aplicación que funcione en todas las plataformas de teléfonos inteligentes, tabletas y de escritorio más populares. Todo lo mencionado aquí ayudó en su ascenso a la popularidad.

2.6.3.3.1. JQuery Mobile 1.4

JQuery Mobile es la forma más fácil de crear sitios y aplicaciones que se puede acceder a todos los dispositivos Tablet, Smartphone y de escritorio más populares. Además jQuery Mobile |.4 es compatible con jQuery |.8 y posteriores.

- **Pplataformas compatibles JQuery Mobile 1.4**

En la siguiente lista se puede observar la compatibilidad de todos los sistemas operativos y exploradores compatibles con esta versión de jQuery Mobile.

Se utiliza un sistema de soporte de la plataforma graduada de 3 niveles: A (completo), B (total menos Ajax), C (HTML básico). La fidelidad visual de la experiencia y la suavidad de las transiciones de página son altamente dependientes de las capacidades de representación de CSS del dispositivo y la plataforma por lo que no toda la experiencia de un grado será de píxel perfecto, pero esa es la naturaleza de la web. (Mobile, 2014)

A-grado - mejor experiencia completa con transiciones de página animadas basadas en Ajax

Apple iOS 4 a 7,0 - Probado en el iPad original (4,3 / 5,0), iPad 2 (4,3 / 5,1 / 6,1), iPad 3 (5,1 / 6,0), iPad Mini (6.1), iPad Retina (7,0), iPhone 3GS (4,3), iPhone 4 (4,3 / 5,1), el iPhone 4S (5,1 / 6,0), iPhone 5 (6,0), y iPhone 5S (7.0)

Android 4.4 (KitKat) - Probado en un Nexus 5

Android 4.1 a 4.3 (Jelly Bean) - Probado en un Nexus Galaxy y Galaxy 7

Android 4.0 (ICS) - Probado en un Nexus Galaxy. Nota: El rendimiento de transición puede ser pobre en *acondicionadas* dispositivos

Android 3.2 (Honeycomb) - Probado en el Samsung Galaxy Tab 10.1 y Motorola XOOM

Android 2.1 a 2.3 -Probado en HTC Incredible (2.2), Droid original (2.2), HTC Aria (2. 1), Google Nexus S (2,3). Funcional en 1.5 y 1.6, pero el rendimiento puede ser lento, probado en Google G1 (1,5)

Windows Phone 7.5-8 - Probado en el HTC Surround (7.5), HTC Trophy (7,5), LG-E900 (7,5), Nokia 800 (7.8), HTC Mazaa (7.8), Nokia Lumia 520 (8), Nokia Lumia 920 (8), HTC 8x (8)

Blackberry 6-1 O - Probado en la Torch 9800 (6) y Style 9670 (6), BlackBerry ® Torch 981 O (7), BlackBerry 21 O (1O)

Playbook Blackberry (1,0-2,0) - Probado en PlayBook

Palm WebOS (1,4-3,0) - Probado en la Palm Pixi (1.4), Pre (1.4), Pre 2 (2.0), HP TouchPad (3.0)

Firefox Mobile 18 - Probado en Android 2.3 y 4.1 dispositivos

Chrome para Android 18 - Probado en Android 4.0 y 4.1 dispositivos

Skyfire 4.1 - Probado en Android 2.3 dispositivo

Opera Mobile 11.5-12 - Probado en Android 2.3

MeeGo 1.2 - Probado en Nokia 950 y N9
Tizen (pre-estreno) - Probado en hardware temprana
Samsung Bada 2.0 - Probado en un Samsung Wave 3, el navegador Dolphin

uc Browser - Probado en Android 2.3 dispositivo

Kindle 3, Fuego, Fuego y HD -Probado en el built-in del navegador WebKit para cada

Rincón de color 1.4.1 -Probado en el original Nook de color, no Nook Tablet
Chrome de escritorio 16-24-Probado en OS X 10.7 y Windows 7
Safari Escritorio 5-6-Probado en OS X 10.8

Firefox de escritorio 10-18 -Probado en OS X 1 o. 7 y Windows 7

Internet Explorer 8 a 10 -Probado en Windows XP, Vista y 7, Windows Surface RT

Opera de escritorio 10-12 - Probado en OS X 10.7 y Windows 7

8-grado - experiencia mejorada, excepto sin las funciones de navegación de Ajax

Opera Mini 7 - Probado en iOS6.1 y Android 4.1
Nokia Symbian r.. 3 -Probado en Nokia N8 (Symbian ^ 3), C7 (Symbian ^ 3), también funciona en N97 (Symbian ^ 1)

C -grado -no mejorada experiencia Basic, HTML que sigue siendo funcional.

Internet Explorer 7 y mayores -Probado en Windows XP
De Apple iOS 3.x en adelante -Probado en iPhone original (3.1), el iPhone 3 (3.2)
Blackberry 5.4 -Probado en el Curve 8330 (4), Storm2 9550 (5), y en negrilla 9770 (5)

Windows Mobile - Probado en el HTC Leo (WinMo 5.2)

Todas las plataformas de teléfonos inteligentes y featurephones mayores – cualquier dispositivo que no admite preguntas de los medios recibirán la experiencia básica de grado C. (Mobile, 2014)

2.6.3.3.2. PhoneGap Cordova

PhoneGap es un marco libre y de código abierto que te permite crear aplicaciones móviles utilizando las API de web estandarizados para las plataformas que le interesan. Se puede utilizar como un contenedor nativo para nuestras aplicaciones móviles. PhoneGap es una distribución de Apache Córdoba. Se puede pensar que en Apache Cordova es como el motor que impulsa PhoneGap, similar a la forma en WebKit que es el motor que impulsa Chrome o Safari.

Para el desarrollo de nuestra aplicación se usará PhoneGap 3.x

2.6.3.4. Sublime Text 2

Sublime Text es un editor de texto sofisticado para el código, marcado y prosa. Esta es una interfaz de marcado, con un extraordinario y rendimiento sorprendente; para un mejor ambiente de trabajo.

2.6.3.5. Modelo COCOMO

Barry Boehm, es un libro sobre economía de la ingeniería de software, introduce una jerarquía de modelos de estimación de software con el nombre de

COCOMO (Constructive, Cost, Model) modelo constructivo de costos. La jerarquía de modelos de Boehm está constituida por lo siguiente:

Modelo I: El modelo COCOMO básico calcula el esfuerzo y el costo del desarrollo de software en función del tamaño del programa, expresado en las líneas estimadas de código (LDC).

Modelo II: El modelo COCOMO intermedio calcula el esfuerzo de desarrollo de software en función del tamaño del programa y en un conjunto de conductores de costos que incluyen la evaluación subjetiva del producto, del hardware, del personal y de los atributos de proyecto. El presente proyecto empleara este modelo.

Modelo III: El modelo COCOMO avanzado incorpora todas las características de la versión intermedia y lleva a cabo una evaluación del impacto de los conductores de costes de cada caso (análisis, diseño, etc.), del proceso de ingeniería de software.

Los modelos COCOMO esta definidos para tres tipos de proyectos de software que son:

1.- Modo orgánico: En este modo, un pequeño grupo de programadores experimentados desarrollan software en un entorno familiar. El tamaño del software varía de unos pocos miles de líneas (tamaño pequeño) a unas decenas de miles de líneas (medio), mientras que en los otros dos modos el tamaño varía de pequeño a muy grandes (varios cientos de miles de líneas).

En este modo, al igual que en los otros, el coste se incrementa a medida que el tamaño lo hace, y el tiempo de desarrollo se alarga.
Se utilizan dos ecuaciones para determinar el esfuerzo de personal y el tiempo de desarrollo. El coste es

$$K_m = 2.4\ S_k^{1.05}$$

Donde K_m se expresa en personas-mes y S_k es el tamaño expresado en miles de líneas de código fuente. El tiempo de desarrollo se da por

$$t_d = 2.5\ K_m^{0.38}$$

Donde K_m se obtiene de la ecuación anterior y t_d es el tiempo de desarrollo en meses. Estas ecuaciones se han obtenido por medio de ajustes de curvas realizado por Boehm en TRW sobre 63 proyectos.

2.- Modo Semiencajado: Es un modo intermedio entre los dos anteriores. Dependiendo del problema, el grupo puede incluir una mezcla de personas experimentadas y no experimentadas.

Las ecuaciones son

$$K_m = 3.0\ S_k^{1.12}$$

Y el tiempo de desarrollo por

$$t_d = 2.5\ K_m^{0.35}$$

3.-Modo empotrado: En este modo, el proyecto tiene unas fuertes restricciones, que pueden estar relacionadas con el procesador y el interface hardware. El problema a resolver es único y es difícil basarse en la experiencia, puesto que puede no haberla.

Las estimaciones de tiempo y coste se basan en las mismas ecuaciones que en el modo orgánico, pero con diferentes constantes. Así, el coste se da por

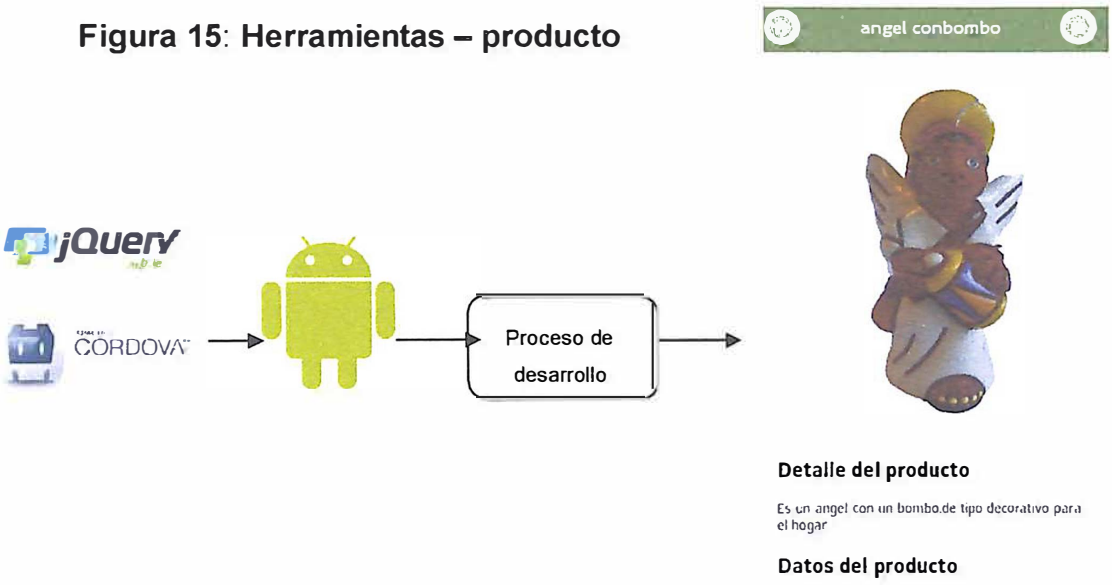
$$K_m = 3.6\ S_k^{1.20}$$

y el tiempo de desarrollo por

$$t_d = 2.5\ K_m^{0.32}$$

2.6.4. Software – Producto

Figura 15: **Herramientas – producto**



Fuente: Elaboración propia.

2.6.4.1. Definición

El software de computadora es el producto que diseñan y construyen los ingenieros de software. Esto abarca programas que se ejecutan dentro de una computadora de cualquier tamaño y arquitectura, documentos que comprenden formularios virtuales e impresos y datos que combinan números, texto, representaciones de información de audio, video e imágenes. (Pressman, 2002)

En este caso se desarrolla un software para dispositivos móviles.

2.6.4.2. Características del software

El software es un elemento del sistema que es lógico, en lugar de físico. A continuación se detallan sus características:

El software se desarrolla, no se fabrica en un sentido clásico. Aunque existen similitudes entre el desarrollo del software y la construcción del hardware, ambas actividades son fundamentalmente diferentes. En ambas actividades la buena calidad se adquiere mediante un buen diseño, pero la fase de construcción del hardware puede introducir problemas de calidad que no existen (o son fácilmente corregibles) en el software. Ambas actividades dependen de las personas, pero la relación entre las personas dedicadas y el trabajo realizado es completamente diferente para el software. Ambas actividades requieren la construcción de un producto pero los enfoques son diferentes. Los costes del software se encuentran en la ingeniería. Esto significa que los proyectos de software no se pueden gestionar como si fueran proyectos de fabricación.

El software no se estropea. Existe una relación de los fallos que el hardware pueda tener en función al tiempo. Esa relación indica que el hardware

exhibe relativamente muchos fallos al principio de su vida (estos fallos son atribuibles normalmente a defectos del diseño o de la fabricación); una vez corregidos los defectos, la tasa de fallos cae hasta un nivel estacionario (bastante bajo, con un poco de optimismo) donde permanece durante un cierto periodo de tiempo. Sin embargo, conforme pasa el tiempo, el hardware empieza a desgastarse y la tasa de fallos se incrementa. El software no es susceptible a los males del entorno que hacen que el hardware se estropee. Por tanto, en teoría, la curva de fallos para el software tendría una similitud a la curva de fallos del hardware, con la diferencia que una vez corregidos los errores al principio del ciclo la curva se estabiliza hasta lograr una función constante. Sin embargo cabe recalcar que el software no se estropea, pero se deteriora, debido a los nuevos requerimientos que el usuario pueda tener.

El software se crea a medida, a medida que la disciplina del software evoluciona, se crea un grupo de componentes de diseño estándar. Los componentes reutilizables se han creado para que el ingeniero pueda concentrarse en elementos verdaderamente innovadores de un diseño, por ejemplo, las partes del diseño que representan algo nuevo. En el mundo del hardware, la reutilización de componentes es una parte natural del proceso de ingeniería. En el mundo del software es algo que sólo ha comenzado a lograrse en una escala amplia. El componente de software debería diseñarse e implementarse para que pueda volver a ser reutilizado en muchos programas diferentes. Los componentes reutilizables modernos encapsulan tanto datos como procesos que se aplican a los datos, permitiendo al ingeniero del software crear nuevas aplicaciones a partir de las partes reutilizables. [PRESSMAN: 2002]

2.6.4.3. Categorías del software

Conforme aumenta la complejidad del software, es más difícil establecer compartimentos nítidamente separados. Las siguientes áreas del software jndican la amplitud de las aplicaciones potenciales:

Software de Sistemas, el software de sistemas es un conjunto de programas que han sido escritos para servir a otros programas. Algunos programas de sistemas procesan estructuras de información compleja pero determinada. Otras aplicaciones de sistemas procesan datos en gran medida indeterminados. En cualquier caso, el área del software de sistemas se caracteriza por una fuerte interacción con el hardware de la computadora o del equipo móvil; una gran utilización por múltiples usuarios; una operación concurrente que requiere una planificación, una compartición de recursos y una sofisticada gestión de procesos; unas estructuras de datos complejas y múltiples interfaces externas.

Software de Tiempo Real, el software que coordina, analiza, controla sucesos del mundo real conforme ocurren, se denomina de tiempo real. Entre los elementos del software de tiempo real se incluyen: un componente de adquisición de datos que recolecta y da formato a la información recibida del entorno externo, un componente de análisis que transforma la información según lo requiera la aplicación, un componente de control y salida que responda al entorno externo, y un componente de monitorización que coordina todos los demás componentes, de forma que pueda mantenerse la repuesta en tiempo real.

Software de Ingeniería y Científico, el software de ingeniería y científico está caracterizado por los algoritmos de manejo de números. Las aplicaciones van desde la astronomía a la vulcanología, desde el análisis de la presión de los automotores a la dinámica orbital de las lanzaderas espaciales y desde la biología molecular a la fabricación automática. Sin embargo, las nuevas aplicaciones del área de ingeniería/ ciencia se han alejado de los algoritmos convencionales numéricos. El diseño asistido por computadora, la simulación de sistemas y otras aplicaciones interactivas, han comenzado a coger características del software de tiempo real e incluso del software de sistemas.

Software basado en Web, las páginas Web buscadas por un explorador son software que incorpora instrucciones ejecutables, y datos. En esencia, la red viene a ser una gran computadora que proporciona un recurso software casi ilimitado que puede ser accedido por cualquiera con un modem o cualquier tipo de conexión a internet.

El propósito principal es dar acceso a la economía Bitcoin y para ello se realizara un prototipo que trabajara de manera general en internet.

3.MARCO PRÁCTICO

3.1. Sistema de transacciones Bitcoin

Como ya vimos en los anteriores capítulos se dio a conocer el marco teórico y conceptual referente al presente trabajo, esto nos proporciona las herramientas necesarias y las bases teóricas para el cumplimiento de los objetivos trazados, vamos a definir el área de trabajo y las tareas que se requieren para desarrollas a construir el sistema de transacciones Bitcoin para la microempresa Cerámicas Jiwasa, cuya finalidad es la de expandir dicha moneda por las diferentes ventajas que esta presenta (BitBoli) y posteriormente incluirlos en un entorno de aplicación web. A este conjunto de tareas se denomina "Proceso de desarrollo de software".

Se señaló que dentro de la elaboración de procesos de software que se utilizan para desarrollar software optamos por la metodología XP para BitBoli, que es un proceso de ingeniería de software que presenta un desarrollo de retroalimentación con coraje para enfrentar los cambios además se adecua para proyectos con requisitos imprecisos y muy cambiantes, y donde existe un alto riesgo técnico, con ello tomamos muy en cuenta que los requisitos pueden ser muy cambiantes y cuya meta es obtener un software de calidad en poco tiempo.

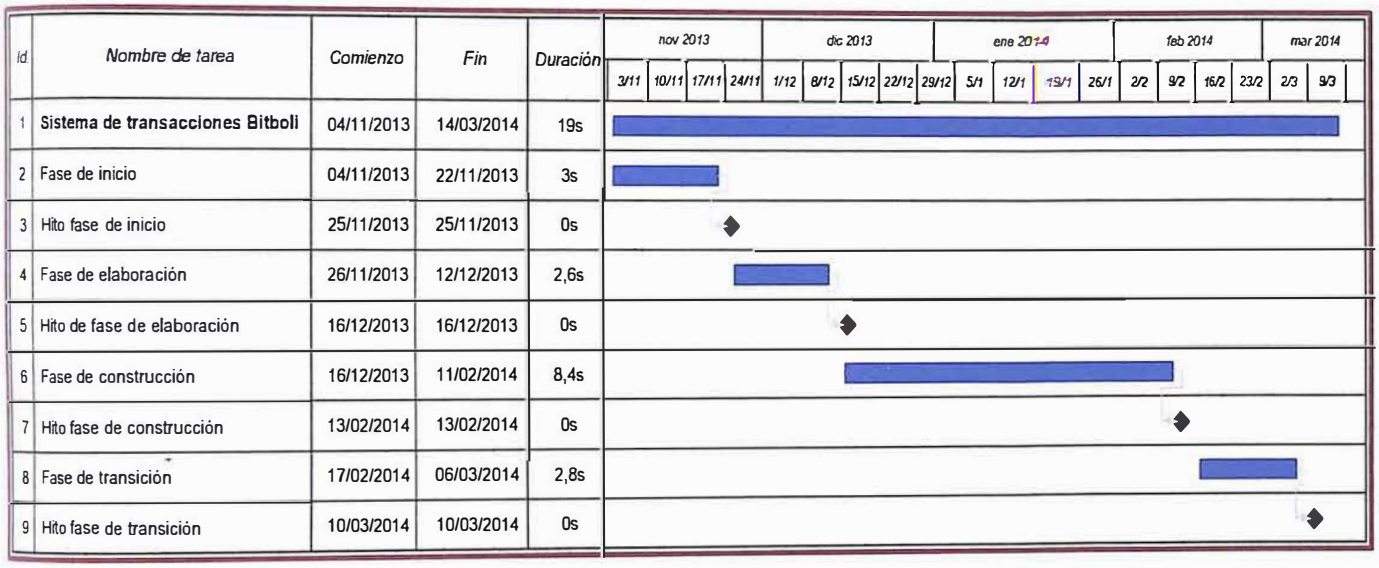
3.1.1. Fase de inicio

una vez que Cerámicas Jiwasa aprobó el inicio de desarrollo de proyecto para desarrollar el sistema de transacciones BitBoli, donde se deben ajustar las actividades, el tiempo y el presupuesto ya estimado.

3.1.1.1. Planificación inicial del proyecto

Definiremos los pasos iniciales de la gestión de proyecto, donde se realizara una planificación acorde con los tiempos de trabajo que se requerirán para la elaboración del proyecto, siguiendo el orden del siguiente cuadro donde se inician actividades:

Figura 16: Diagrama de Gantt



Id	Nombre de tarea	Comienzo	Fin	Duración
1	**Sistema de transacciones Bitboli**	04/11/2013	14/03/2014	19s
2	Fase de inicio	04/11/2013	22/11/2013	3s
3	Hito fase de inicio	25/11/2013	25/11/2013	0s
4	Fase de elaboración	26/11/2013	12/12/2013	2,6s
5	Hito de fase de elaboración	16/12/2013	16/12/2013	0s
6	Fase de construcción	16/12/2013	11/02/2014	8,4s
7	Hito fase de construcción	13/02/2014	13/02/2014	0s
8	Fase de transición	17/02/2014	06/03/2014	2,8s
9	Hito fase de transición	10/03/2014	10/03/2014	0s

Fuente: Elaboración propia.

Tabla 3: Plan de actividades para el sistema de transacciones BitBoli

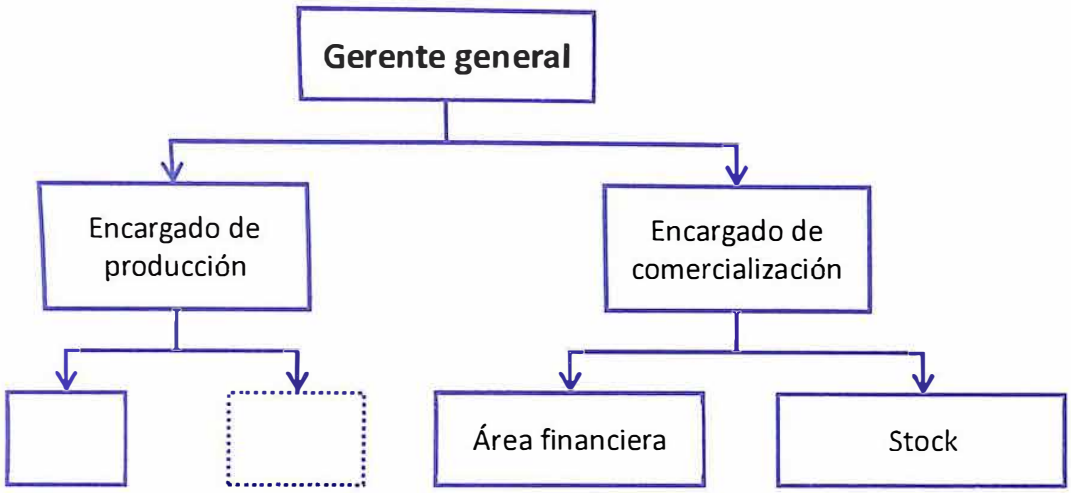
HITO	ACTIVIDAD	SEMANA	ITERACIÓN
Inicio: el hito que marca el fin de esta etapa es el plan de desarrollo.	Planificación inicial del proyecto.	1	1
	Organización del proyecto.	1	1
	Modelo de casos de uso de negocio	1	1
	Análisis de factibilidad	1	1
	Lista de requerimientos	1-2	1
	Realizar diagramas de casos de uso	2	1
	Describir diagramas de casos de uso	2	1
Elaboración: este es el hito que define el diseño final del sistema.	Realizar el modelo de procesos	3	1
	Describir los procesos	4-5	1
	Realizar el diagrama de secuencias	6	1
	Realizar el diagrama de clases	6	1
	Realizar el diagrama de estados	6	1
Construcción: en este hito se desarrollara el prototipo.	Desarrollo de prototipo	7-13	1-2
	Generar repositorio de datos	8-10	1-2
	Diseño grafico	12-14	1
Transición: el hito de esta instancia es la presentación del prototipo a la institución.	Completar el desarrollo de producto final realizando los ajustes necesarios.	15-18	1
	Pruebas de las transacciones	18-19	1

Fuente: Elaboración propia.

3.1.1.2. Análisis micro-empresarial

3.1.1.2.1. Organigrama

Figura 17: Organigrama de la microempresa Cerámicas Jiwasa



Fuente: Elaboración propia.

3.1.1.2.2. Descripción del organigrama de la micro – empresa

Por lo que tenemos la siguiente descripción:

- **Gerente general:** Es la máxima autoridad de la microempresa Cerámicas Jiwasa, todas las decisiones importantes deben estar avaladas por el gerente general.

- **Encargado de producción:** Es el encargado principal del área de producción en sus diferentes procesos en cuanto al producto se refiere.

- **Encargado de comercialización:** Es el encargado directo de entregar los productos a los clientes mayoristas ésta cuenta con dos subdivisiones el *Stock y el área financiera.*

- **Stock:** Esta área permite informar al encargado de comercialización, el tiempo de entrega una vez que esl stock cuente con lo requerido.

- **Área financiera:** Esta área es la encargada de realizar las transacciones al momento que los clientes efectúan el pago a la microempresa, muchas veces el gerente general es a quien los clientes efectúan el pago.

3.1.1.2.3. Descripción de transacciones de la microempresa Cerámicas Jiwasa

Actualmente la microempresa cuenta con trabajos HECHO EN BOLIVIA, los cuales son exportados al exterior del país mediante intermediarios o son enviados de manera directa, en ambos casos se debe acceder a una cuenta bancaria la que por naturaleza la denominamos 'tercero de confianza' en este caso el banco, quien necesariamente cobrara una comisión del dinero enviado, presentando así desventaja para el microempresario porque recibe el neto de la mercadería menos el cobro del envío por ello no percibe el total de lo enviado; además que al momento de realizar la transacción el tipo de cambio de la divisa suele ser variante.

3.1.1.2.4. Análisis de factibilidad

Existen técnicos excelentes para la comparación de costos beneficios del sistema propuesto.

Al momento de realizar la estimación se toma en cuenta no solo el procedimiento, sino que también se toma en cuenta los recursos, costos y planificación. El tamaño del proyecto es otro factor importante que puede afectar la precisión y las estimaciones. A medida que el tamaño aumenta, crece rápidamente la dependencia entre varios elementos de software.

Para que el proyecto sea considerado como factible debe pasar por lo menos las siguientes pruebas, de no ser así el proyecto no es factible.

3.1.1.2.5. Modelo COCOMO (Modelo constructivo de costes)

A diferencia de tiempos anteriores hoy en día el software se constituye en el elemento más caro en los sistemas informáticos. E tiempo que se contabiliza es de ocho meses aproximadamente, este tiempo es corroborado por el modelo COCOMO posteriormente, si suponemos una jornada de ocho horas diarias de trabajo.

Tabla 4: Matriz de coeficiente COCOMO

Nivel / Modo	Básico		Intermedio	
	a_i	b_i	a_i	b_i
Orgánico	2.4	1.05	3.2	1.05
Semiencajado	3.0	1.12	3.0	1.12
Empotrado	3.6	1.2	2.8	1.2

Fuente: Modelo Cocomo 'http://www.sc.ehu.es/jiwdocoj/cocomo.htm'

Las bases para el empleo de COCOMO II es el costo de esfuerzo de desarrollo de software estimado luego de determinar la arquitectura del sistema.

Como se puede observar (tabla anterior), se tiene la matriz de coeficientes COCOMO, para los diferentes modos y niveles, se tiene los diferentes estándares de complejidad de esfuerzo del personal como en el caso del básico que varía de 2.4 a 3.6 según la complejidad del proyecto.

A continuación realizaremos una aplicación en este modelo COCOMO II en el proyecto con el modo Orgánico.

Exponente $b_i = 1.05$ este puede variar hasta un máximo 1.2.

Donde K_m se obtiene de la siguiente operación y t_d que es el tiempo de desarrollo en meses.

El coste es: $K_m = 2.4 * S_k^{1.05} = 2.4 * (0.8)_k^{1.05} = 1.8 \approx$ **2 personas /mes**

Donde S_k representa el tamaño expresado en miles de código, para el caso particular se determina 1,5 líneas aproximadamente.

El tiempo de desarrollo se da por: $t_d = 2.5\ K_m^{0.38} = 2.5 * (2)_m^{0.38}$

T_d= 3 meses

El cuál es el tiempo requerido para el desarrollo de software del sistema.

3.1.1.2.6. Análisis costo beneficio

El análisis costo beneficio nos permite sumar el valor de los beneficios y restar los gastos recurrentes, esporádicos y periódicos. Este análisis se lo realizara en relación al tiempo determinado para el desarrollo. En nuestra planificación seria la parte de desarrollo de software, es decir la fase de construcción.

Este análisis se lo realizara de una manera mucho más subjetiva, dando valores a los costos y los beneficios intangibles o inexactos en nuestro proyecto. Muchos de los elementos usados tendrán un valor por inauguración o suposición. Los costos de este sistema se distribuyen de la siguiente manera:

Tabla 5: Análisis costo – beneficio recursos humanos

Descripción	Nro. De personas	Tiempo en horas	Costo por hora	Costo por día	Costo total
Análisis	1	320	Bs. 20	Bs. 160	Bs. 6,400
Programación	2	640	Bs. 15	Bs. 120	Bs. 9,600
Diseño	1	40	Bs. 12	Bs. 96	Bs. 480
Instalación	2	20	Bs. 8	Bs. 64	Bs. 160
Transacciones Bitboli	2	20	Bs. 8	Bs. 64	Bs. 160
					Bs. 16,800

Fuente: Elaboración propia.

Tabla 6: Análisis costo – beneficio Equipo

Descripción	Cantidad	Costo mensual	Costo	Costo total
Dispositivo móvil	2	0	Bs. 1,000	Bs. 2,000
Servicio de internet	1	Bs. 250		Bs. 250
				Bs. 2,250

Fuente: Elaboración propia.

Dispositivo móvil: Se requerirán dos dispositivos móviles que en este caso con Sistema operativo Android como mínimo con la versión 3.2; uno se usara para las transacciones directas con el cliente y si el usuario así lo requiere el segundo servirá como un dispositivo de almacenamiento de los Bitcoin.

Servicio de internet: el siguiente servicio será usado de manera mensual adquiriendo un servicio mensual de Viva 4G teniendo como mínima la tarifa 250 que permitirá tener 250 Mg por mes.

Tabla 7: Análisis costo – beneficio total

Costo de:	Valor
Recurso humano	Bs. 16,800
Equipo y servicio	Bs. 2,250
Costo total del proyecto	Bs. 19,050

Fuente: Elaboración propia.

El costo total presentado es una inversión a disminuir el coste de transacciones para la microempresa además damos la oportunidad de realizar las transacciones P2P y con ello damos el inicio al propósito de expandir dicha moneda y el fin de dar acceso al mercado global Bitcoin de nuestro proyecto.

3.1.1.2.7. Factibilidad operacional

El uso de elementos de hardware no es obstáculo para la operación de parte del gerente o encargado de las transacciones ya que el celular es un medio conocido.

El sistema tiene un diseño amigable y ordenado que permite al cliente realizar la compra y pago de tal forma que pueda guiarse fácilmente.

3.1.1.2.8. Análisis de costo por transacción en Bolivia

Para el siguiente análisis tomamos en cuenta las tarifas por transacción, con terceros de confianza en Bolivia. Como referencia de dichos datos tomamos en cuenta los siguientes bancos BCP (Banco de crédito), Banco FIE, BNB (Banco nacional de Bolivia), Tigo Money y entidades más conocidas con el servicio de transacciones a nivel internacional Western Unión y PayPal.

Tabla 8: Referencia del costo en una transacción

Nombre de la entidad	Límite del monto a enviar	Comisión	Pre requisitos
Banco Nacional de Bolivia *BNB*	Bs. 1 a Bs. 7,070	Bs. 142	Ser cliente del banco.
	Mayores a Bs. 70,701	1.2 %	
Banco FIE	Hasta $us 50,000	$us 60	Ser cliente del banco.
	$us 50,001 a $us 200,000	1.05%	
Tigo money (P2P)	Bs. 1 hasta Bs. 900	Ctv. 0,20	Tener activa una línea Tigo(http://www.tigo.com.bo/tigo-money/preguntas-frecuentes)
	Bs. 901 hasta Bs. 1,800	Bs. 10	
Western Union	$us 1 a $us 60	5 %	Sin tener cuenta o afiliación a Western Union.
	$us 1,000.01 a $us 7,500.00	**4 %**	
Paypal	**NS**	**2.5 % Ó 3,4% + €0,35 EUR**	**Sin costo a la apertura de una cuenta**

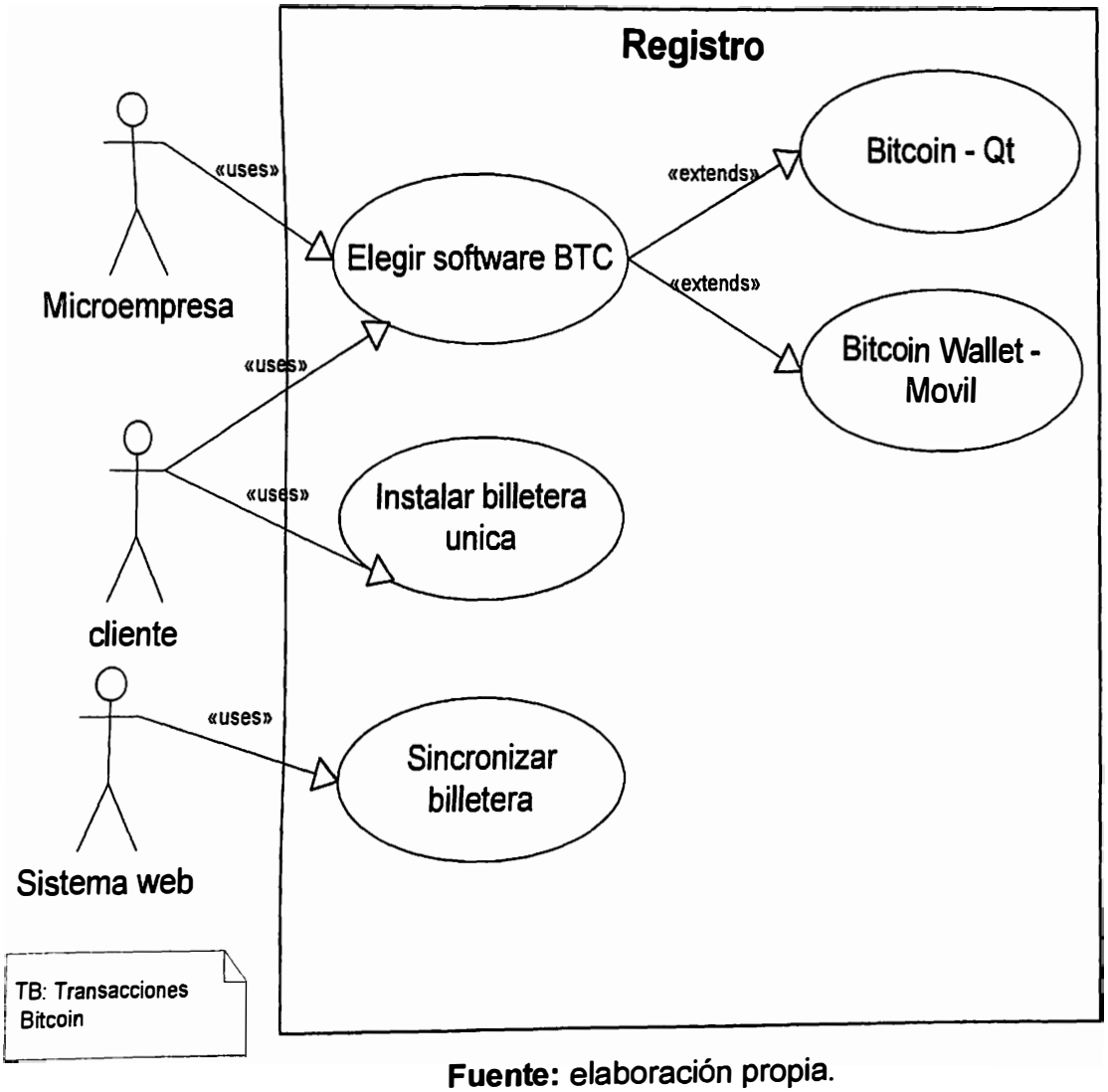
Fuente: Datos obtenidos a través de los datos proporcionados en línea de las diferentes entidades.

3.1.1.3. Diagrama de Casos de Uso

3.1.1.3.1. Diagrama de Casos de Uso – Registro de TB

Figura 18: Diagrama de casos de uso – Registro

CU – 001



Fuente: elaboración propia.

Tabla 5: Descripción de CU 001– Registro

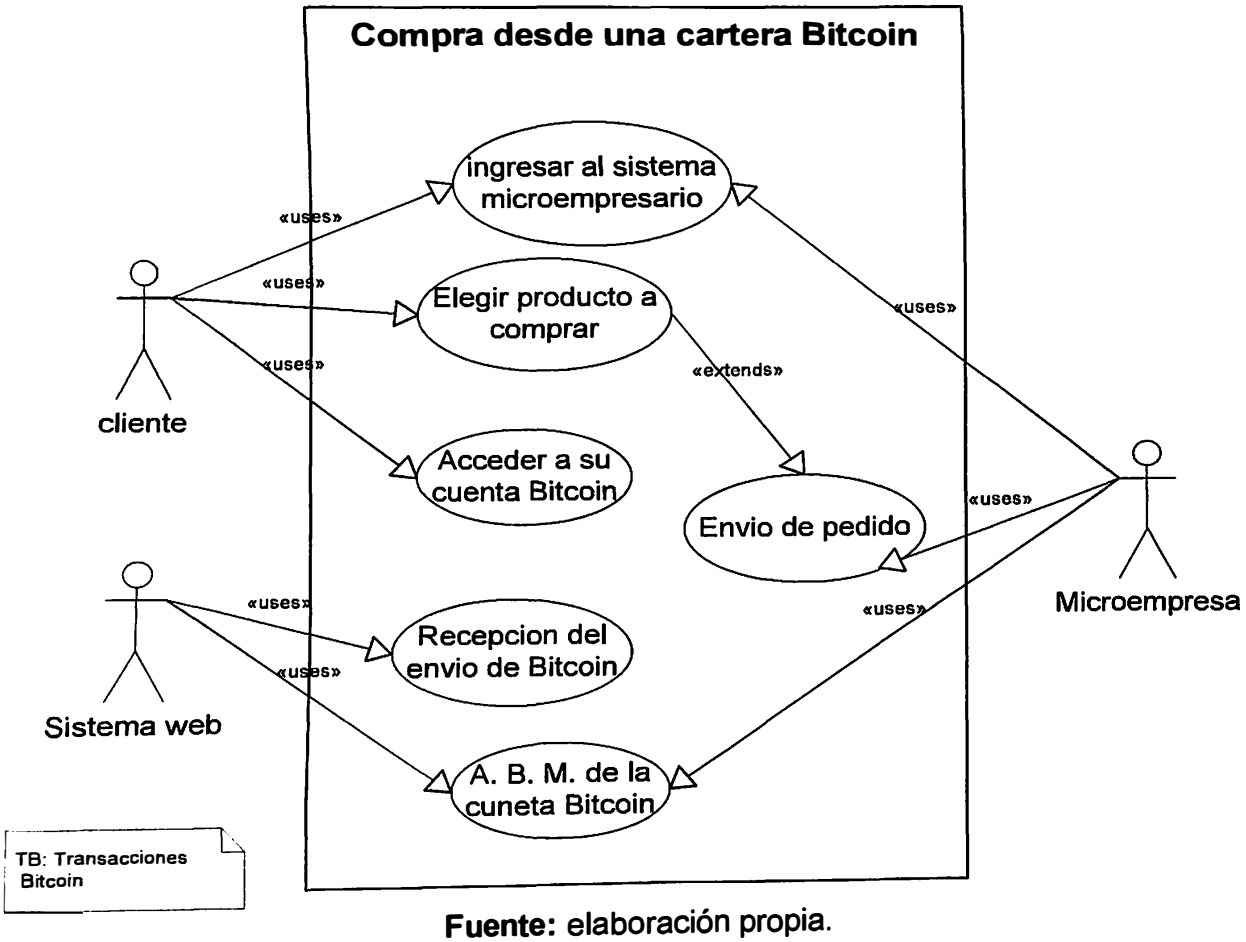
CU – 001	**Registro**
Descripción	Antes de comenzar a usar el Bitcoin se debe instalar Bitcoin Wallet u otro de acuerdo al dispositivo y tener conexión a internet, según se describe en el siguiente caso de uso.
Secuencia normal	1.- El usuario instala la cartera. 2.- Inicia sesión desde su cartera (propio banco). 3.- La red Bitcoin asigna un código alfanumérico, único. 4.- El usuario debe sincronizar la cadena (La sincronización puede durar hasta dos días).
Excepciones	La sincronización depende mucho de la velocidad de internet o la frecuencia de tener en línea a la cartera.

Fuente: Elaboración propia.

3.1.1.3.2. Diagrama de Casos de Uso – Compra desde una cartera Bitcoin

Figura 19: Diagrama de casos de uso – Compra desde una cartera Bitcoin

CU - 002



Fuente: elaboración propia.

Tabla 9: Descripción de CU 002 – Compra desde una cartera BTC

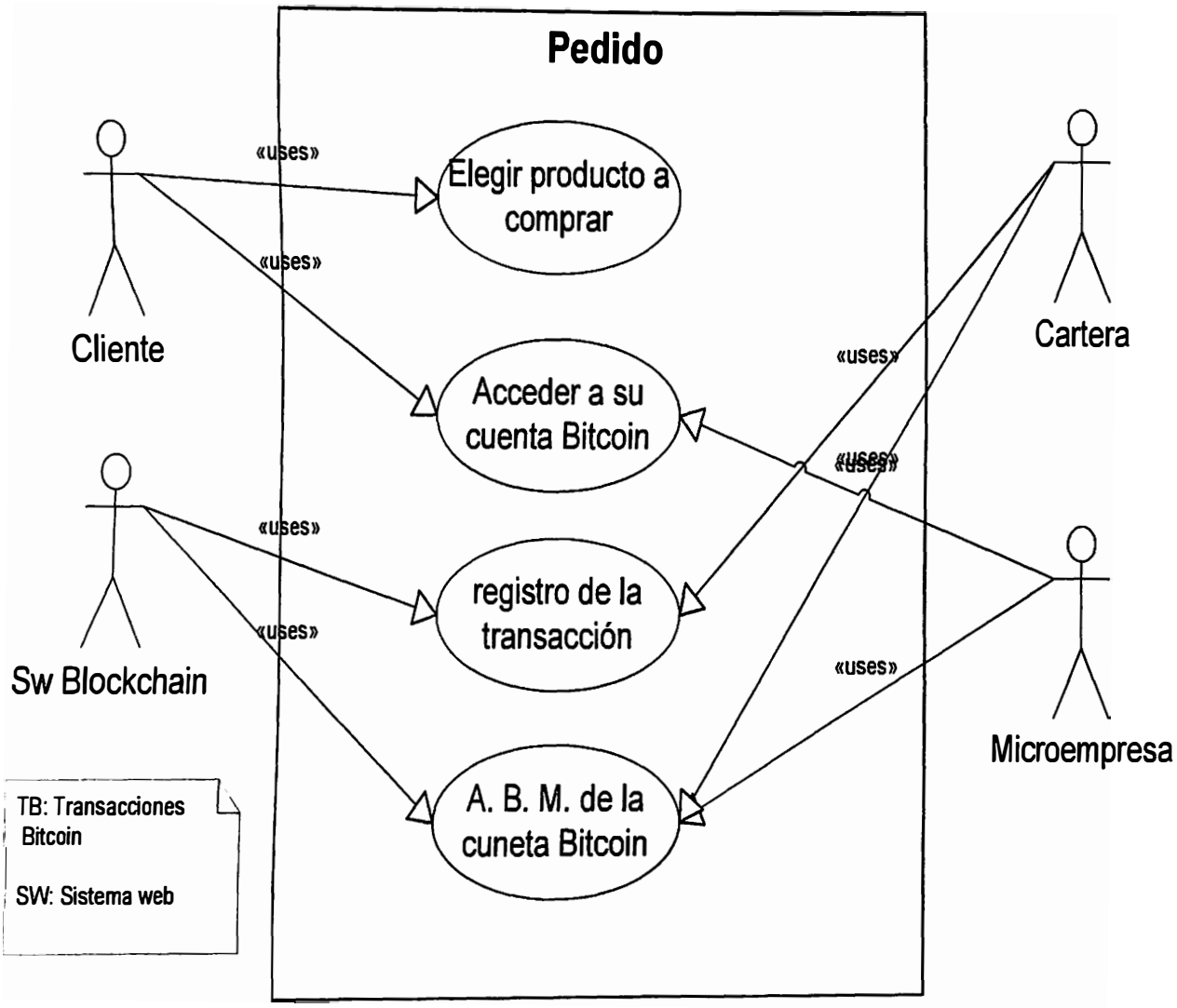
CU – 002	**Comprar desde una cartera Bitcoin**
Descripción	El sistema deberá permitir realizar transacciones desde el dispositivo en donde se instaló previamente Bitcoin Wallet, la compra – venta se la realizara con conexión a internet, según se describe en el siguiente caso de uso.
Secuencia normal	1.- El usuario inicia sesión desde su Bitcoin Wallet. 2.- El usuario selecciona la función a realizar. 3.- La red Bitcoin verifica si la cuenta tiene Bitcoins. 4.- Si la cartera cuenta con Bitcoin entonces el sistema verifica la transacción a realizar, comprobando que la transacción no sea duplicada. 5.- Se realiza transacción.
Excepciones	De no ser así, no se realiza la transacción.

Fuente: Elaboración propia.

3.1.1.3.3. Diagrama de casos de Uso – Hacer pedido

Figura 20: Diagrama de casos de uso – Hacer pedido

CU - 003



Fuente: elaboración propia.

Tabla 10: Descripción de CU 003 - Pedido

CU – 003	**Pedido**
Descripción	El pedido antecede a la compra por lo tanto la cartera "Bitcoin Wallet" debe estar en ejecución tanto como para enviar y recibir Bitcoin según se describe en el siguiente caso de uso.
Secuencia normal	1.- El usuario inicia sesión desde su cartera. 2.- Selecciona la función a realizar. 3.- La red Bitcoin verifica si la cuenta tiene Bitcoin. 4.- Se realiza transacción.
Excepciones	De no ser así, no se realiza la transacción.

Fuente: Elaboración propia.

3.1.1.4. Requerimientos del usuario

Los requerimientos más importantes para realizar el sistema son:

- ❖ Conocer el valor del Bitcoin con relación a otras divisas.
- ❖ Tener fácil acceso a los productos de la microempresa.

3.1.1.5. Requerimientos de funcionamiento

Los requerimientos anteriores se pueden reflejar en el desarrollo diferenciado de los siguientes módulos:

- Módulo de venta
  - Búsqueda del pedido.
  - Carrito de compras.
  - Realizar pedido.
- Módulo de transacción
  - Acceder a la cartera Bitcoin.
  - Realizar transacción

3.1.2. Fase de elaboración

En esta fase se construye el diseño de la arquitectura que deberá evolucionar hasta perfeccionarse como nuestro sistema final.

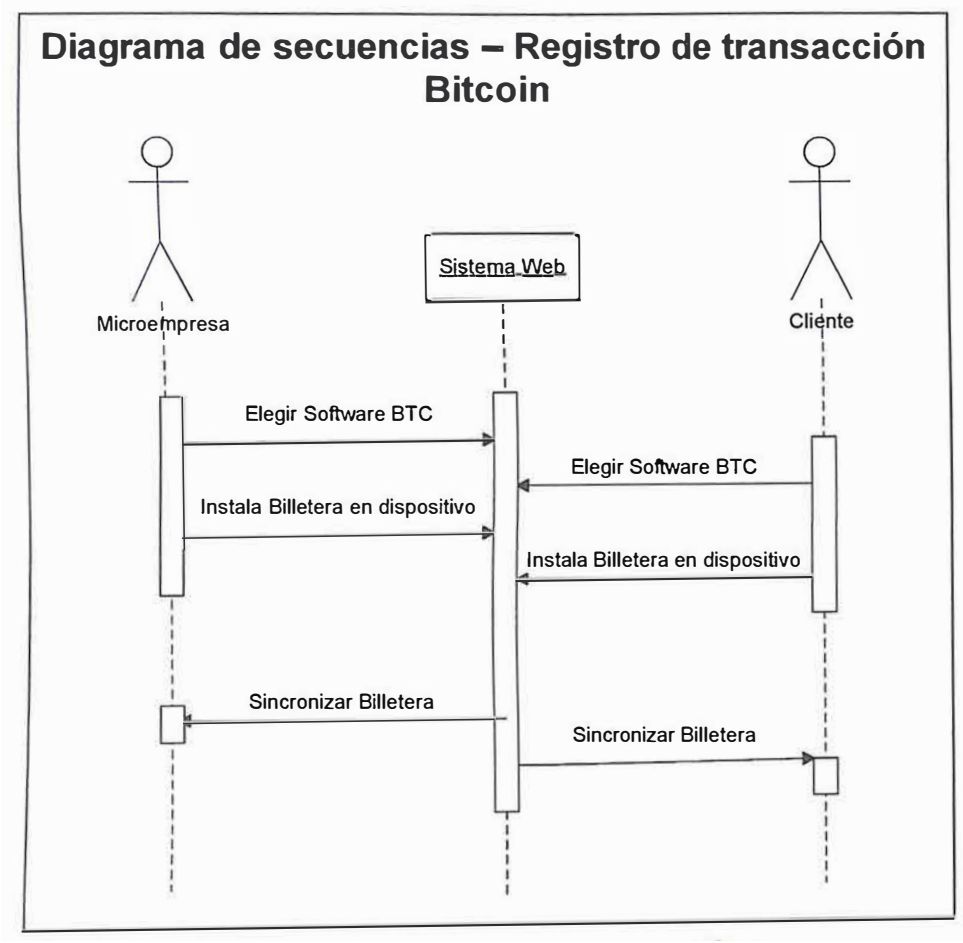
3.1.2.1. Modelo de análisis y diseño

A continuación se muestran unos cuadros de los procesos que han sido utilizados para analizar, documentar y mejorar las transacciones sin intermediarios en el mercado micro empresarial.

3.1.2.2. Diagrama de secuencias

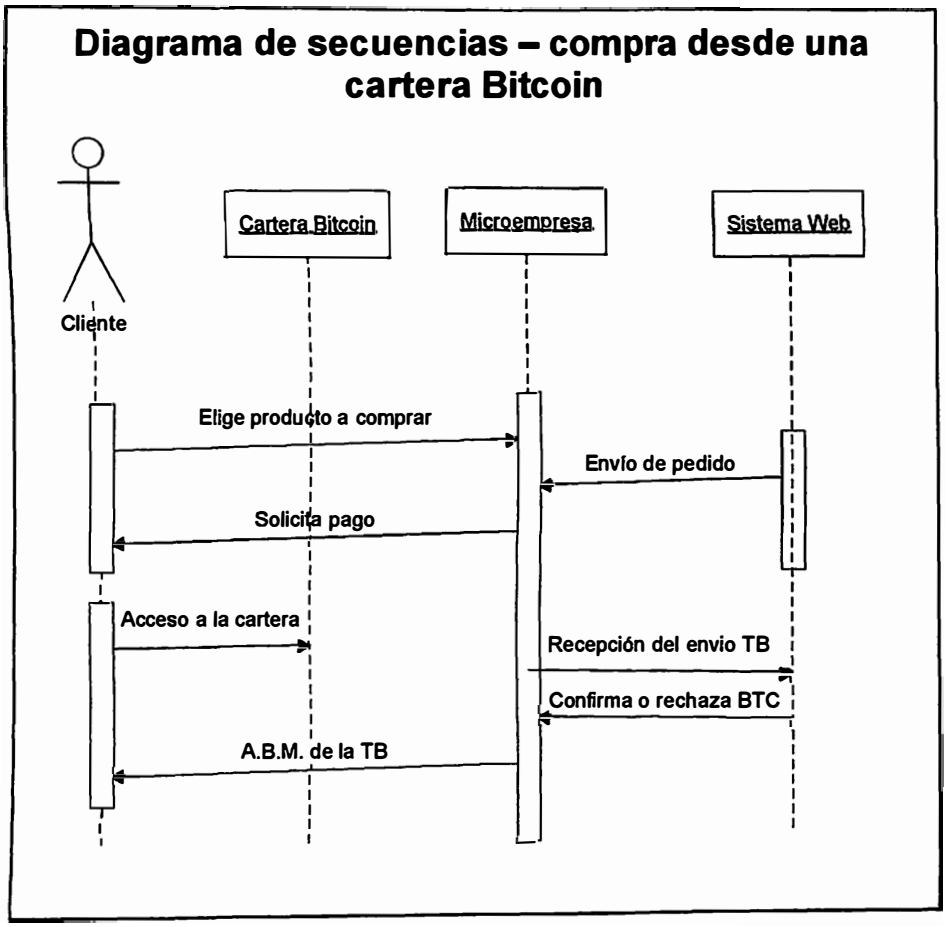
3.1.2.2.1. Diagramas de secuencias registro de TB

Figura 21: Diagrama de secuencia - registro de transacciones BTC



3.1.2.2.2. Diagramas de secuencias compra desde una cartera Bitcoin

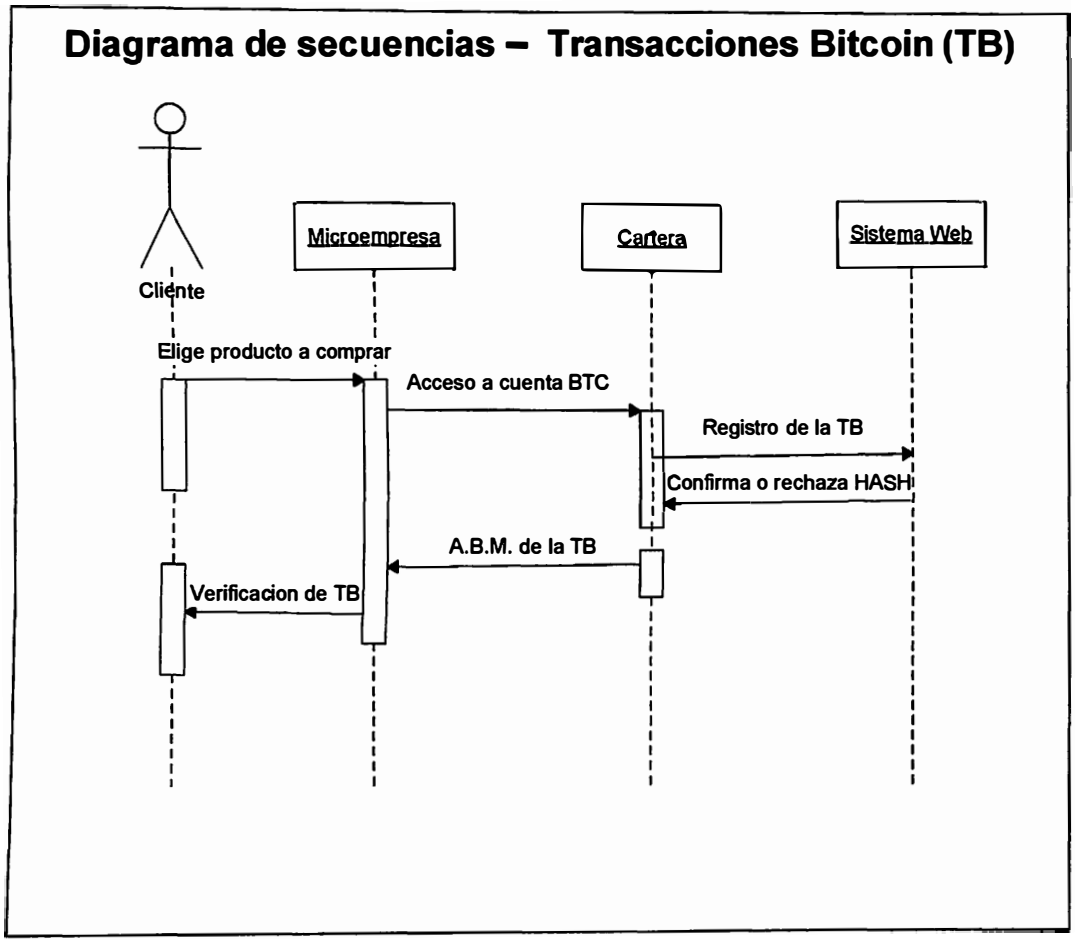
Figura 22: Diagrama de secuencia de Compra desde una cartera Bitcoin



Fuente: Elaboración propia.

3.1.2.2.3. Diagramas de secuencias Transacción Bitcoin

Figura 23: Diagrama de secuencia de transacciones Bitcoin



Fuente: Elaboración propia.

3.2. Bitboli (Bitcoin en Bolivia)

Después de haber seguido una estricta investigación en la que basaremos las transacciones Bitcoin, podemos nuevamente retomar el proceso de adaptación en cuanto al entorno a la fase de construcción.

3.2.1. Billetera para el ordenador Bitcoin – Qt

Bitcoin es un protocolo, un software y una moneda digital, que permite:

- Pagos en todo el mundo
- Transacciones instantáneas punto a punto
- Bajos o cero costos de procesamiento

Bitcoin utiliza tecnología punto a punto para operar sin una autoridad central; gestionando las transacciones y la emisión de Bitcoin que se llevan a cabo conjuntamente por la red. A través de muchas de sus propiedades únicas, Bitcoin permite usos interesantes que no pueden ser cubiertos por otros sistemas de pago.

El software es un proyecto libre de código abierto, impulsado por la comunidad y liberado bajo la licencia MIT.

- **Licencia MIT**

Esta licencia concede permiso de forma gratuita a cualquier persona que obtenga la copia de un determinado software y archivos de documentos asociados con el software sin restricciones de usar, copiar, modificar, fusionar, publicar, distribuir, sub licenciar o vender copias del software.

EL SOFTWARE SE ENTREGA 'TAL CUAL", SIN GARANTÍA DE NINGÚN TIPO, EXPRESA O IMPLÍCITA, INCLUYENDO PERO NO LIMITADO A LAS GARANTÍAS DE COMERCIALIZACIÓN, IDONEIDAD PARA UN PROPÓSITO PARTICULAR Y NO INFRACCIÓN. EN NINGÚN CASO, LOS

AUTORES O TITULARES DEL COPYRIGHT SERÁN RESPONSABLES DE NINGUNA RECLAMACIÓN, DAÑO U OTRA RESPONSABILIDAD, YA SEA EN UNA ACCIÓN DE CONTRATO, AGRAVIO O CUALQUIER OTRA FORMA, DERIVADOS DE, DE O EN CONEXION CON EL SOFTWARE O EL USO U OTROS TRATOS EN EL SOFTWARE. (opensource)

3.2.1.1. Requerimientos

Sistema operativo Linux, Windows o Android (Preferentemente Windows homer - el cual se usara para este proyecto)

3.2.1.2. Descargar Billetera

- Ir a la dirección http://bitcoin.org/es/descargar

Figura 24: Pagina de descarga de la Billetera Qt

Fuente: El Bitcoin (http://bitcoin.org/es/descarga)

- A continuación ir a la carpeta, que en este caso es la siguiente dirección: C:\Users\MELENDREZ\Downloads\bitcoin-0.8.3-win32-setup.

3.2.1.3. Instalación

- Ubicar archivo.
- Hacer doble click y acontinuacion comenzara la instalación.

Figura 25: Pantalla de ubicación del archivo para instalar

Fuente: Captura de pantalla de la instalación de la Cartera BTC

3.2.2. Monedero en línea "Blockchain"

Este monedero es una cuenta Bitcoin en línea que se puede utilizar para hacer pagos en todo el mundo de manera gratuita. Este servicio te permite pagar con Bitcoin de manera sencilla y segura ya sea desde tu teléfono móvil u ordenador.

Blockchain.info no es un banco sencillamente se conserva la completa propiedad del dinero. Por lo que además nos indica en la

página https://blockchain.info/es/wallet, que Blockchain.info no puede ver su saldo, transacciones o realizar pagos en su nombre.

3.2.2.1. Creación de cuenta en Blockchain.info

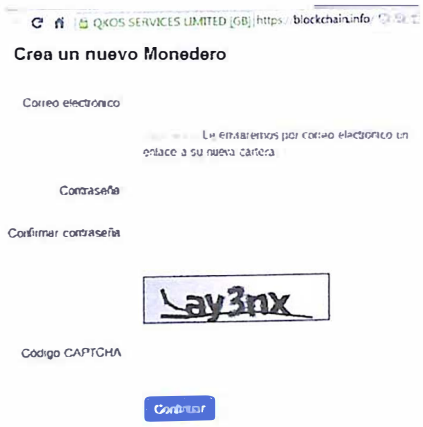
Paso 1: https://blockchain.info/es/wallet

Figura 26: Página oficial de Blockchain

Fuente: Captura de pantalla de Blockchain

Después de haber hecho click sobre **crear cuenta,** llenamos los siguientes datos.

Figura 27: Llenar datos página Blockchain



Fuente: Blockchain.info

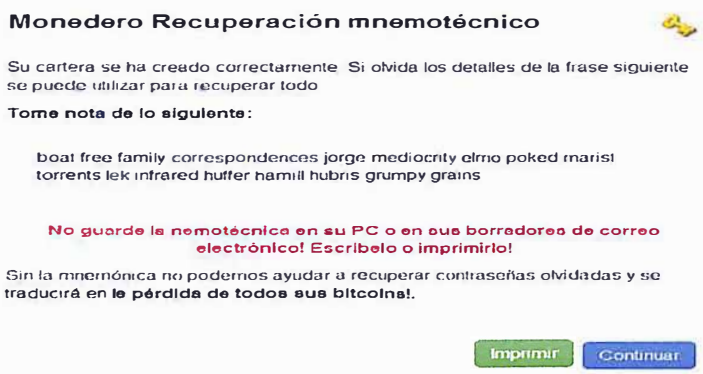
Paso 2: Cuando llenamos todos los datos a continuación, emerge un comunicado que debe tomarse muy en cuenta.

Figura 28: Advertencia de Blockchain

Fuente: Blockchain.

Y a continuación lo siguiente es una posibilidad con la cual puedas recuperar tu cuenta en caso de olvidar la contraseña de tu monedero. Donde indica:" Su cartera se ha creado correctamente. Si olvida los detalles de la frase siguiente se puede utilizar para recuperar todo."

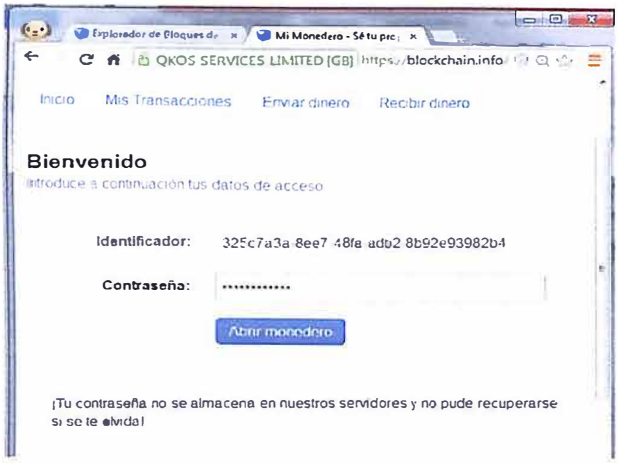
Figura 29: En caso de olvidar contraseña de Blockchain



Fuente: Blockchain.

Paso3: Iniciamos sesión en nuestro monedero.

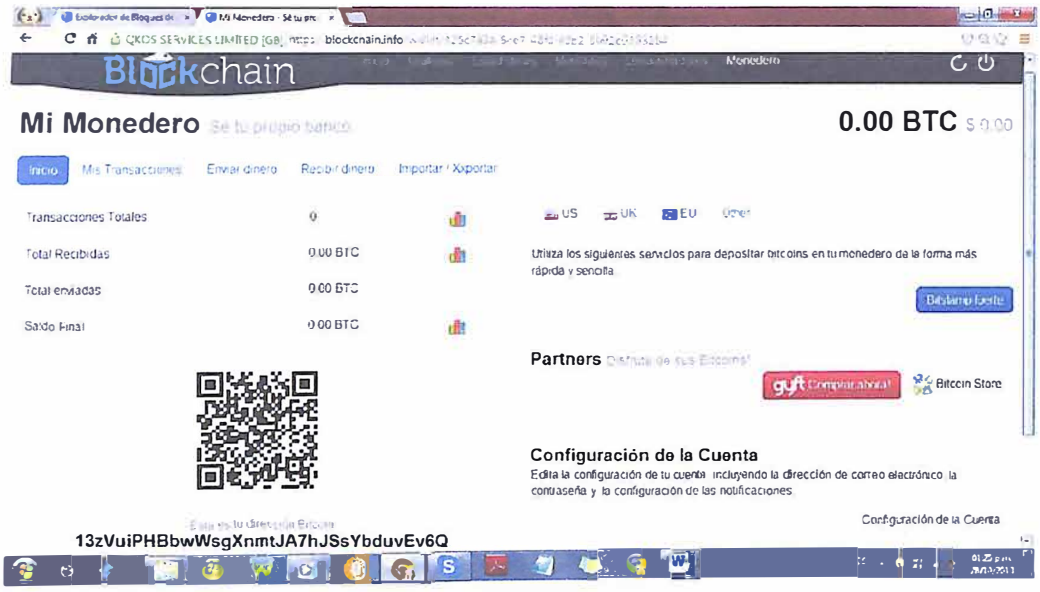
Figura 30: Iniciar sesión en Blockchain



Fuente: Blockchain.

Una vez iniciado sesión de Blockchain, podemos apreciar la siguiente pantalla.

Figura 31: Después de iniciar sesión en Blockchain



Fuente: Blockchain.

3.2.3. Bitcoin Wallet - Billetera móvil

Esta es una cartera de Bitcoin para tu dispositivo Android, donde se puede enviar Bitcoin entre teléfonos haciendo explorar los códigos QR que muestra la aplicación o mediante NFC con sus siglas en ingles Mear Field Communication.

3.2.3.1. Requerimiento

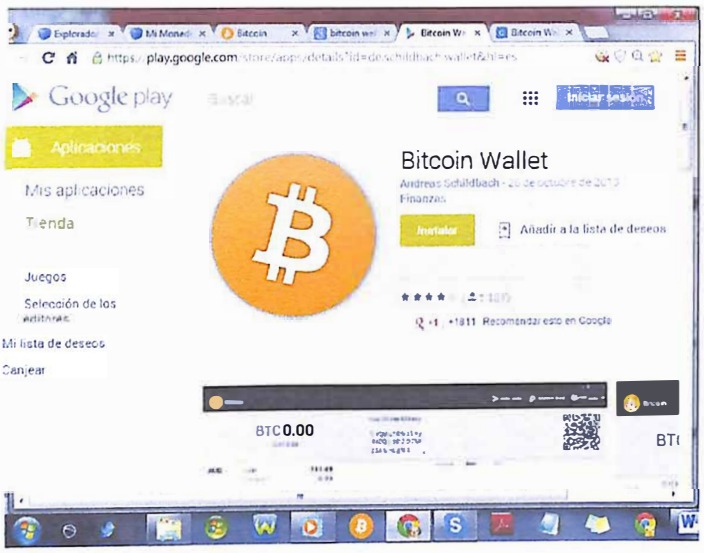
Sistema operativo Android (Preferentemente versiones superiores a Android 2.3.7 - el cual la versión de Android mencionado será utilizada para este proyecto).

3.2.3.2. Descarga de Bitcoin Wallet

La billetera la descargamos de la siguiente dirección:

https://play.google.com/store/apps/details?id=de.schildbach.wallet&hl=es

Figura 32: Pagina de descarga de la billetera Bitcoin Wallet



Fuente: Google Play.

3.2.3.3. Instalación

- Ejecutar el archivo apk en el dispositivo móvil.
- A continuación se observara una primera vista de la siguiente captura de pantalla del dispositivo.

Figura 33: Billetera móvil Bitcoin Wallet

Fuente: Captura de pantalla Bitcoin Wallet

3.2.4. Creación de prototipo Bitboli

3.2.4.1. Creación del espacio de desarrollo

- **Requerimientos**
  - ✓ Eclipse
  - ✓ Sistema operativo Windows (preferentemente Windows 7)
  - ✓ Jquery Mobile
  - ✓ Cordova (Phonegap)
  - ✓ Sublime Text 2

3.2.4.1.1. Crear nuevo documento

Primero debemos instalar el compilador de Java y la máquina virtual (http://www.oracle.com/technetwork/java/javase/downloads/index.html y http://developer.android.com/sdk/index.html)

El segundo paso es la descarga del ADT (que contiene todo lo necesario para comenzar el desarrollo de aplicaciones en Android), lo hacemos del sitio (descargar el de 32 o 64 bit según el JDK de Java que ya tenemos instalado del paso anterior): Android SDK. En la siguiente dirección, http://developer.android.com/sdk/index.html

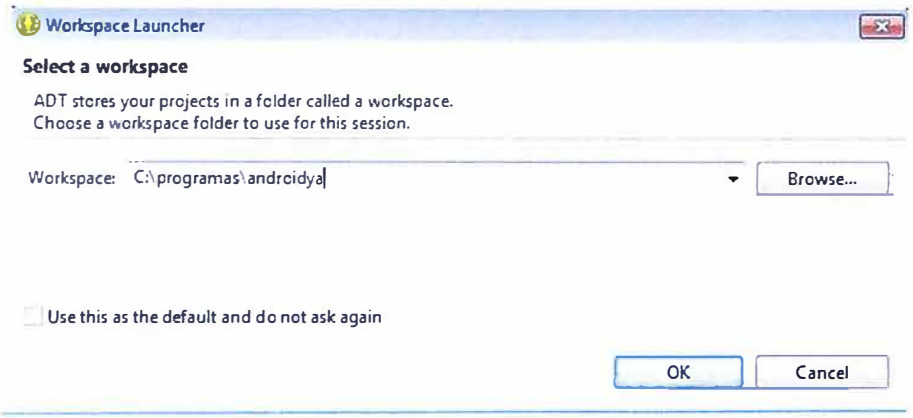
El tercer paso es descomprimir el ADT y luego ejecutamos el Eclipse

Figura 34: Descomprimir el ADT y ejecutar el Eclipse

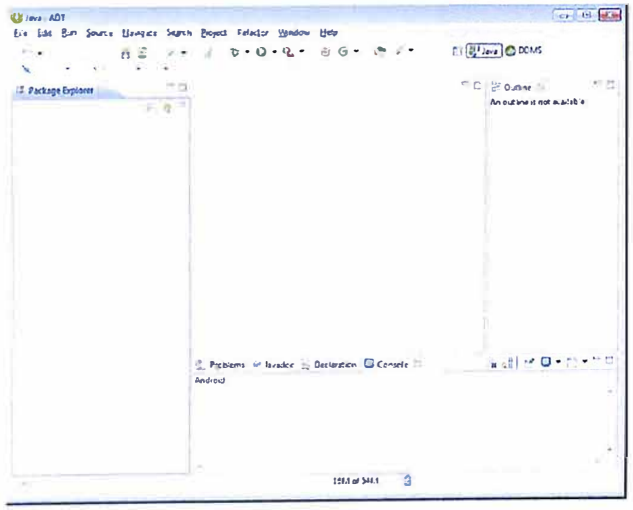
Fuente: Captura de pantalla al momento de la instalación

Direccionamos el almacenamiento de los proyectos que desarrollemos:

Figura 35: Pasos para la instalación del entorno de trabajo

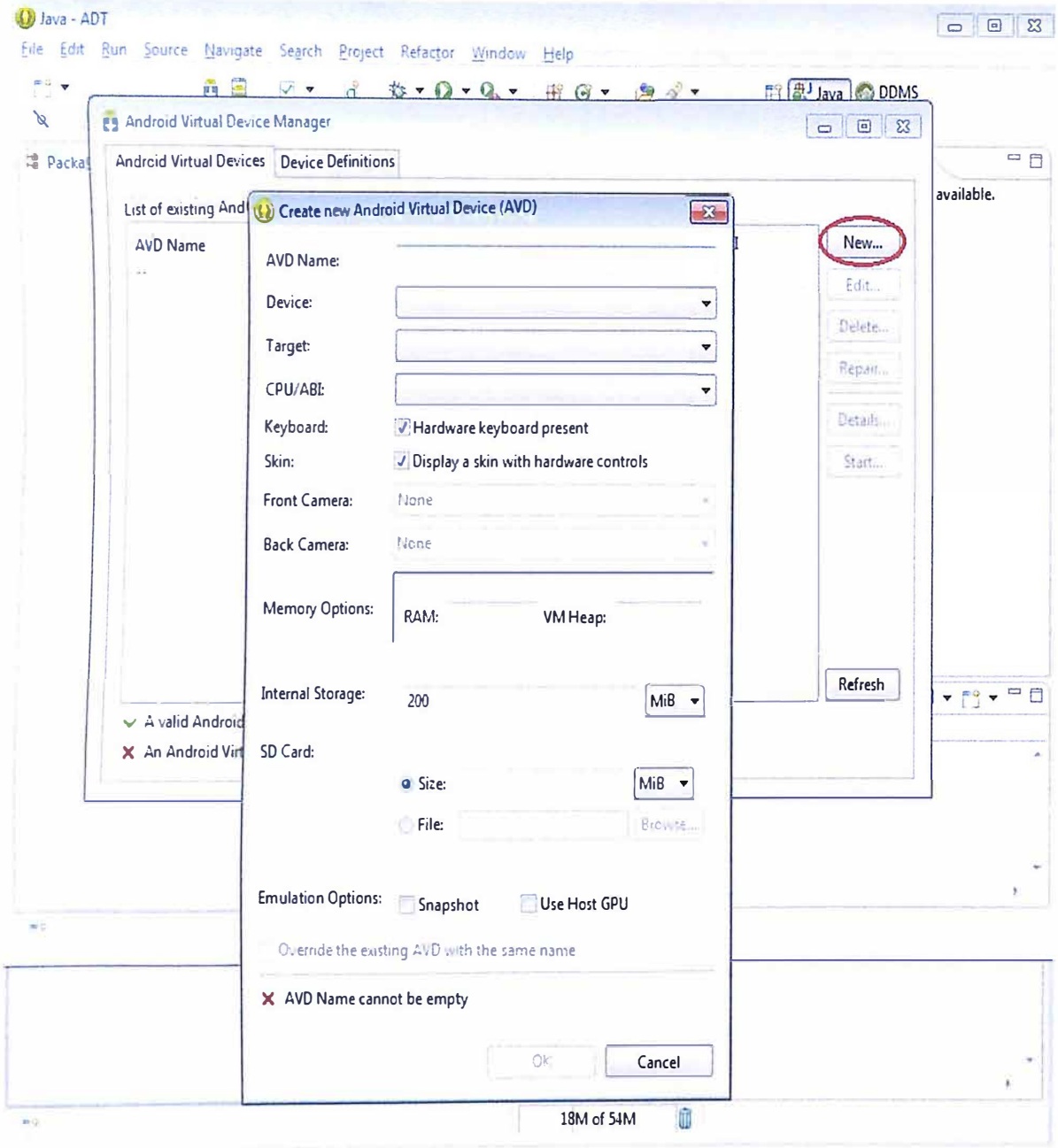


A continuación el entorno de trabajo:

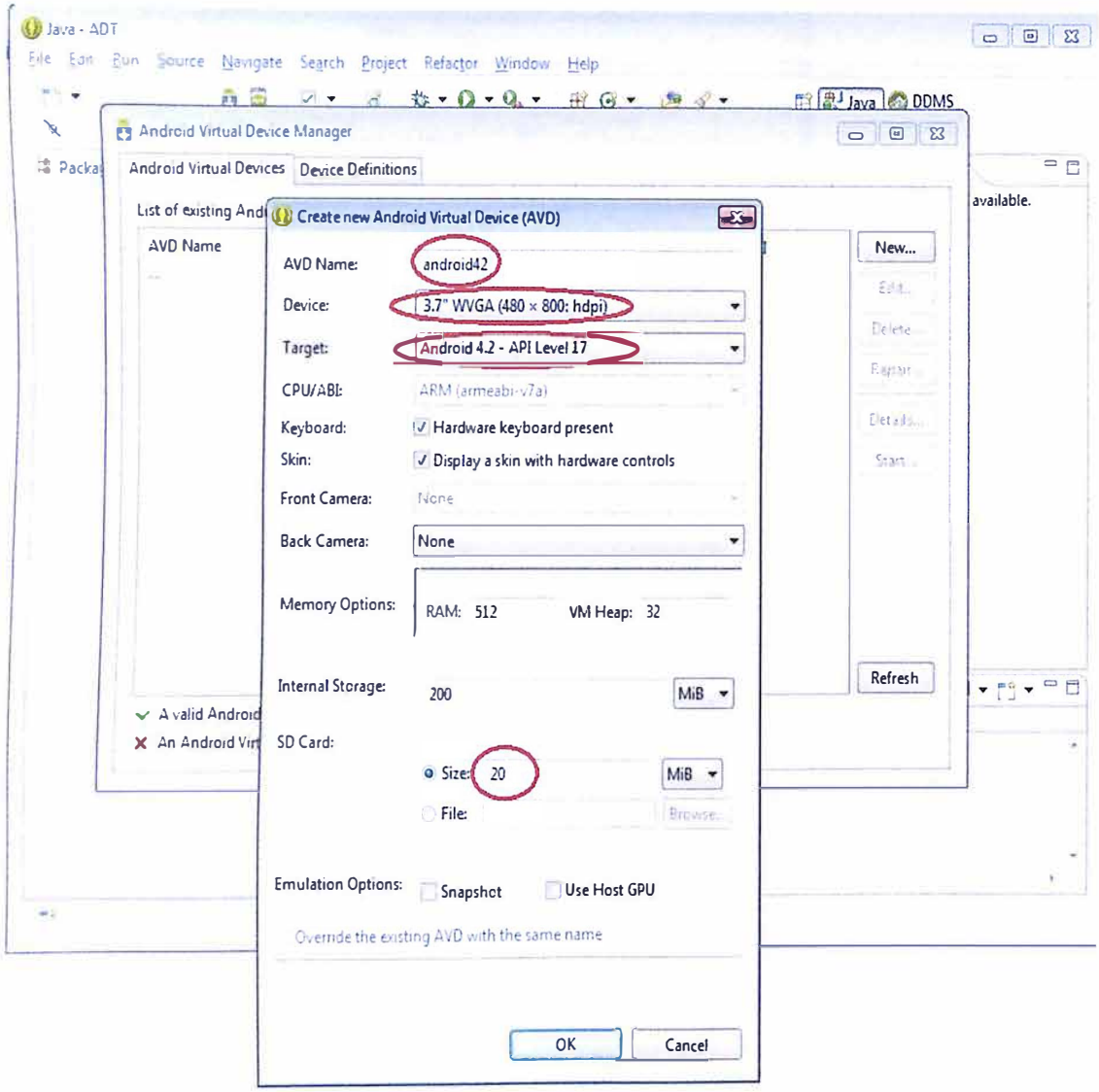


Por último debemos crear el AVD (Android Virtual Device) para ello nos dirigimos a la opción Window -> Android Virtual Device Manager.

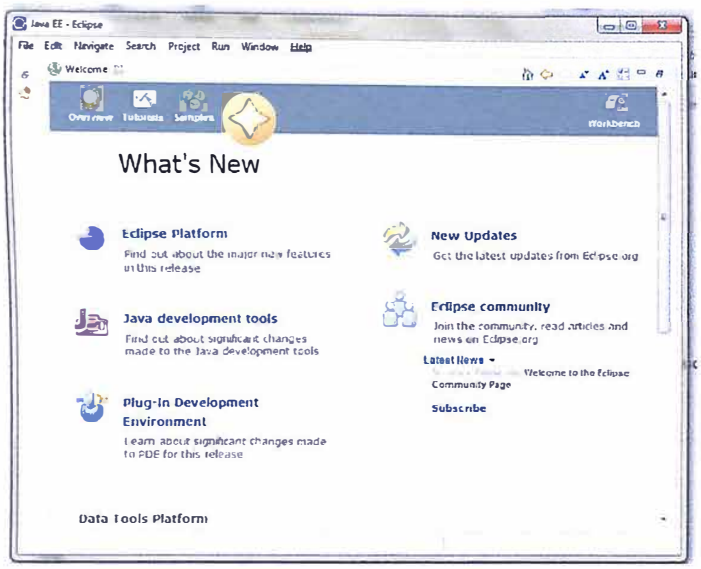
En este diálogo debemos crear el emulador de Android (presionamos el botón New...):

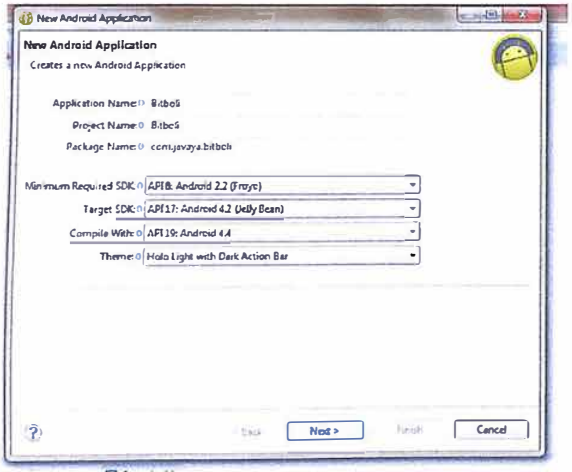


En este diálogo asignamos un nombre a nuestro AVD, elegimos un dispositivo (que no sea tan grande ya que no entrara en pantalla, podemos probar con WVGA (480,800)), lo enlazamos con la versión de SDK respectivo, fijamos un tamaño al SD Card:



Ya tenemos todo configurado para el desarrollo de aplicaciones Android.





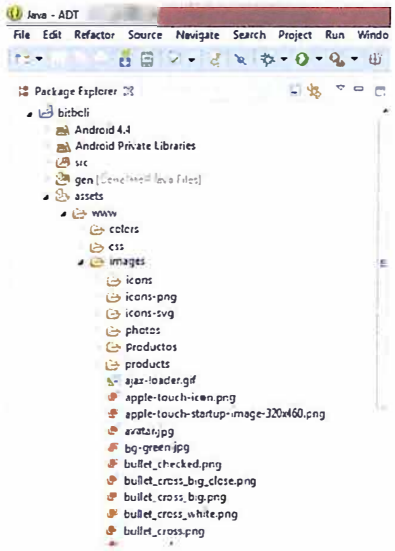
El ADT nos genera todos los directorios y archivos básicos para iniciar nuestro proyecto:

Figura 36: App del documento creado

Fuente: Captura de pantalla del documento creado.

3.2.4.1.2. Archivo de imágenes

Figura 37: Ubicación de la dirección de las imágenes



Fuente: Captura de pantalla del documento creado.

- **Diseño grafico**

Para seguir con la línea grafica al momento de hacer trabajar con el carrito de compras y la interfaz de compra y venta para el cliente además hacer la demostración de las transacciones Bitcoin; se han utilizado imágenes tomadas de la microempresa Cerámicas Jiwasa. Las imágenes fueron copiadas a la carpeta

H:\bitboli\assets\www\images\products

El resultado final está basado en un carrito de compras por lo que el sistema da la posibilidad de realizar transacciones con el dinero digital Bitcoin llamando así a esta aplicación Bitboli.

4. PROPUESTA

4.1. Aplicación Bitboli

A continuación la planificación se mostrará gráficamente el resultado del trabajo realizado durante todos estos meses, según el planteamiento en el diagrama de Gantt en la planificación de este proyecto.

Además se mostraran las imágenes del sistema Bitboli en sus dos funciones importantes las transacciones Bitcoin y el uso del sistema Bitboli.

Figura 38: Icono de la aplicación Bitboli

Referencia: Captura de pantalla del icono de la aplicación Bitboli.

Figura 39: Página principal de la aplicación

Referencia: Aplicación Bitboli

Tenemos seis burbujitas en las que encontramos información acerca del Bitcoin, en la primera burbuja encontramos información acerca de ***Que es el Bitcoin*** como muestra la Figura 14.

Figura 40: contenido del primer enlace *Acerca de*

Acerca de la aplicación

¿Qué es BitBoli?

Bitboli es una aplicación de compra la cual usa la moneda virtual **bitcoin**. Esta es una de las primera de las aplicaciones con estas características desarrolladas en **Bolivia**. Ya que Bitcoin presenta diferentes ventajas en cuanto a moneda digital se refiere. esta aplicación esta dirigida al sector micro empresario de Bolivia.Como fin se plantea dar acceso al mercado global Bitcoin. De tal manera el propósito se expandir el uso del dinero virtual Bitcoin debido a las diferentes ventajas que nos trae el simple hecho de usar las monedas virtuales.

¿Qué es Bitcoin?

Bitcoin es una moneda digital P2P desregulada y descentralizada, la que fue ideada por una persona (o un grupo) anónimo bajo el seudónimo de Satoshi Nakamoto en 2009, quien explicó en un artículo las bases de su moneda electrónica con la siguiente descripción:

"Una versión 100% P2P de dinero electrónico que le permitiría a los pagos online ser enviados directamente de un ente a otro ***sin pasar a través de una institución financiera*** *(...) eso si. este beneficio se pierde si se necesita de un tercero que verifique la transacción confirmando que el dinero electrónico no se usó previamente* (más conocido como doble-gasto. lo que evita la falsificación)".

Referencia: Aplicación Bitboli

En esta página podemos ver un video acerca de Bitcoin que de manera sencilla y clara, da a conocer ciertos aspectos de Bitcoin.

Si queremos volver a la parte de atrás tocamos el botón de atrás del dispositivo o si queremos ir directamente a la página principal tocamos el globito de la parte superior izquierda.

Figura 41: Botón de acceso a la página de inicio de la aplicación Bitboli

Referencia: Aplicación Bitboli

Además del botón de la parte superior existe otro en la parte superior derecha *Figura 16*.

Figura 42: Botón de acceso a la página de a comprar

Referencia: Aplicación Bitboli

Que nos ayuda a ver la lista de ***detalles de compras*** una vez que se realiza la selección de ***productos*** a comprar (que a continuación describimos).

Figura 43: Pagina de productos

Referencia: Aplicación Bitboli

La página de productos almacena más de 40 productos los mismos que son apilados de una columna de 10 productos y si queremos seguir viendo más productos podemos elegir la opción **ver más elementos.** Cuando vemos algún producto de interés podemos tocar la pantalla en el lugar del producto (si el dispositivo es touch) y a continuación tendremos más detalle del producto, además el precio y el botón *comprar.*

Cuando elegimos la opción *comprar,* dicho producto forma ya parte del carrito de compras que lo denominamos *Detalles de compras.*

Figura 44: Página de detalle y datos del producto

Referencia: Aplicación Bitboli.

Una vez que elegimos una serie de productos a *comprar*, tenemos la página *detalles de compras,* donde encontramos el total a pagar y el botón **confirmar.**

Figura 45: Pagina detalle de compras

Referencia: Aplicación Bitboli

Una vez que confirmamos la compra, la aplicación Bitboli realizara la transacción desde la cartera móvil del dispositivo a la cuenta de la microempresa Cerámicas Jiwasa.

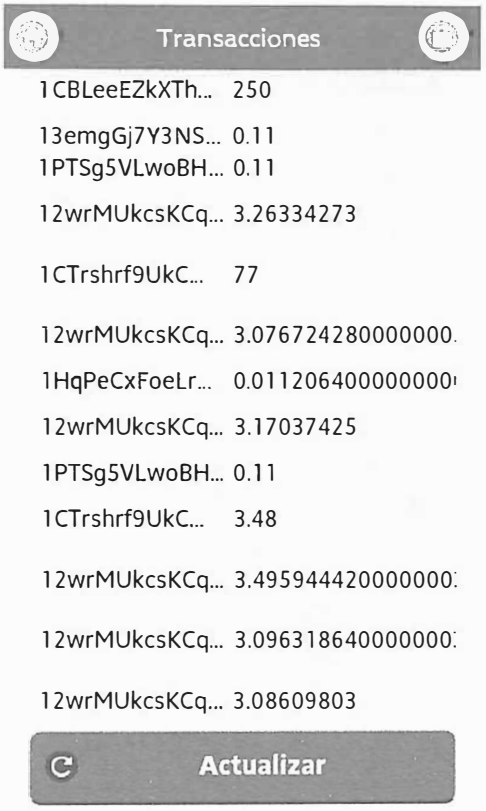
Luego tenemos la cuarta burbuja *tipo de cambio,* la misma que nos muestra el valor del Bitcoin en moneda Boliviana y el valor en Dólares, que además podemos actualizar dicha información con el botón *actualizar.*

Figura 46: Página tipo de cambio

Referencia: Aplicación Bitboli

La penúltima burbuja contiene datos denominados *transacciones* donde encontramos las últimas transacciones realizadas en la red Bitcoin, para la comprobación de dicha transacción al momento de realizar la operación.

Figura 47: Página de transacciones



Referencia: Aplicación Bitboli

Y por último encontramos la burbuja de *contactos* donde el cliente puede contactarse para tener más información acerca de la Microempresa Cerámicas Jiwasa.

Figura 48: Página de contactos

Referencia: Aplicación Bitboli

Además de tocar la parte del celular el dispositivo trasladara el número de celular al teléfono listo para realizar la llamada.

Figura 49: Enlace desde la aplicación Bitboli a el teclado del celular

Referencia: Aplicación Bitboli

La cartera bitcoin del dispositivo móvil debe estar previamente instalada ya que al realizar alguna transacción es desde los archivos de la cartera Bitcoin que se las realizaran, además debe verificar que la transacción ha sido realizada, viendo su cartera Bitcoin.

Figura 50: Página de Bitcoin

Referencia: Captura de pantalla de Bitcoin Wallet.

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Una vez realizada el Sistema denominado ***Bitboli*** podemos concluir que aparte de desarrollar el sistema como tal, se ha logrado el desarrollo de los módulos de seguimiento de la economía Bitcoin para mantener informado a su operador, con referente al precio BTC y las transacciones recientes, el módulo de productos donde se tienen todos los productos de la microempresa, el modulo Carrito donde se tiene los detalles de los productos y el módulo de contactos donde el cliente podrá contactarse con el proveedor, comprendido la definición de Moneda digital y los funcionamientos de cada componente, tal es el caso de Bitcoin un medio de pago seguro y accesible.

Al trabajar con Bitcoin se han realizado pruebas de transacciones con micro Bitcoin, los mismos que fueron depositadas en diferentes carteras y se puedo comprobar la velocidad de envío y de recepción de dicha transacción.

En la utilización del RUP como metodología de desarrollo de software hemos resuelto el Realizar el análisis, diseño y desarrollo del sistema BITBOLI de acuerdo a los requerimientos de un usuario de Bitcoin y las características que un microempresario necesita para vender su producto.

Las facilidades que ofrece el eclipse como entorno de trabajo para Java y su relación con desarrollo de aplicaciones Android, nos permitió desarrollara la aplicación con las diferentes características.

Las facultades de nuestro sistema permite al los clientes comprar con Bitcoin y al microempresario vender con dicha moneda; además la aplicación Bitboli puede ser base para que otras micro empresas puedan adaptarse este sistema.

Finalmente para el diseño y desarrollo del Sistema Bitboli por el que se siguió los procesos necesarios para que el resultado sea un producto de buena calidad, utilizando metodologías adecuadas y lenguajes de programación modernos; de tal manera que los microempresarios puedan acceder al mercado global.

5.2. Recomendaciones

En general se puede decir que el sistema de Cartera móvil digital de dinero digital bitcoin para microempresas bolivianas, denominado Bitboli, puede ser posible gracias a la utilización de dicha moneda en diferentes negocios, la cual puede ser contener aplicaciones que nos relaciones con Bitcoin.

La creación de políticas que incentiven el uso de esta moneda a microempresarios, puede hacer que Bitboli se convierta en la herramienta ideal para la cual fue diseñada.

Además se busca que nuestra aplicación sea conocida internacionalmente con el desarrollo de aplicaciones similares a lo planteado, para que nuestro propósito sea realizado.

6. BIBLIOGRAFÍA Y WEBGRAFÍA

Ableson, Frank. 2013. DeveloperWorks. [En línea] 05 de Febrero de 2013. [Citado el: 26 de Agosto de 2013.] http://www.ibm.com/developerworks/ssa/library/os-android-devel/.

BCB. 2014. *El dinero electrónico en Bolivia.* La Paz : Publicacion mensual, 2014. N° 4 Año 2 May 2014.

Bilitelia. 2012. Bilitelia. [En línea] 16 de junio de 2012. [Citado el: 23 de Septiembre de 2012.] http://bitelia.com/2011/06/bitcoin-eeuu.

Bitcoin, En. 2012. hash; En Bitcoin. *En Bitcoin.* [En línea] 2 de Agosto de 2012. [Citado el: 14 de Octubre de 2012.] https://en.bitcoin.it/wiki/Hash.

Bitcoinmagazine. 2012. Bitcoinmagazine. [En línea] 2 de Agosto de 2012. [Citado el: 14 de Octubre de 2012.] http://Bitcoinmagazine.com .

Castro, Luis. 2013. About.com. [En línea] 01 de enero de 2013. [Citado el: 26 de Agosto de 2013.] http://aprenderinternet.about.com/od/Glosario/g/Que-Es-Html-5.htm.

Desdeelexilio. 2012. Desde el exilio. [En línea] 4 de junio de 2012. [Citado el: 04 de junio de 2012.] http://www.desdeelexilio.com/2012/06/04/comprendiendo-la economia-capitulo-16-la-teoria-cuantitativa-del-dinero/.

Eabolivia. 2011. eabolivia. [En línea] 16 de agosto de 2011. [Citado el: 22 de octubre de 2012.] http://www.eabolivia.com/economia/4695-bolivia-y-venezuela-implementan-moneda-virtual-sucre.html.

El Diario. 2012. El Diario. [En línea] 02 de julio de 2012. [Citado el: 24 de octubre de 2012.] http://www.eldiario.net/noticias/2012/2012_07/nt120702/ciencia.php?n=1&-facebook-ya-no-tendra-su-propia-moneda.

Elbitcoin. 2011. El Bitcoin. El Bitcoin en español. [En línea] 27 de mayo de 2011. [Citado el: 15 de diciembre de 2012.] http://elbitcoin.org/que-es-un-bitcoin/.

Elbitcoin. 2011. http://elbitcoin.org/que-es-un-bitcoin/. http://elbitcoin.org/que-es-un-bitcoinl. [En línea] 2012 de mayo de 2011. [Citado el: 28 de octubre de 2012.] http://elbitcoin.org/que-es-un-bitcoin/.

EnBitcoin. 2012. Nonce en bitcoin. en Bitcoin. [En línea] 2 de agosto de 2012. [Citado el: 14 de octubre de 2012.] https://en.bitcoin.it/wiki/Nonce.

Fiduciario, Dinero. 2012. Wikipedia. Wiki. [En línea] Wikipedia.org, 28 de octubre de 2012. [Citado el: 13 de diciembre de 2012.] http://es.wikipedia.org/wiki/Dinero_fiduciario.

Fundaempresa. 2011. Fundaempresa. [En línea] 14 de junio de 2011. [Citado el: 18 de septiembre de 2012.] http://www.fundempresa.org.bo/docs/content/enero_ 461.pdf.

Infobae. infobae. [En línea] [Citado el: 24 de octubre de 2012.] http://www.infobae.com/notas/599923-Bitcoins-la-nueva-moneda-virtual. html.

Jacobson, Booch Rumbaugh. 2000. El proceso unificado de desaffollo de software. Madrid : Addison Wesley, 2000.

José Antonio Córdova. 2012. Sistemas de pagos electrónicos. El primer salario. La Paz - Bolivia : Unifranz, 2012. Vol. 111, 3.

Kristoufek, Ladislav. 2014. What are the main drivers of the Bitcoin price? Evidence from wavelet coherence analysis. s.l. : arXiv, 2014. 1406.0268v1.

Krohn, Artus y Sorge, Christoph. 2012. Practica/ Aspects of the Bitcoin System. Germany: s.n., 2012.

Laumas, Guarcharan S. 1968. the degree of moneyness of savings deposits. s.l.: the American Economic Review, 1968. págs. 501-503.

Lopez, Juan Torrez. 2009. Como crean los bancos el dienro (y poder). MANU ROBLES-ARANGIZ INSTITUTUA, 2009.

Mexía, Fernando. 2009. El plumilla. [En línea] 25 de mayo de 2009. [Citado el: 24 de octubre de 2012.] http://www.elplumilla.net/2009/05/25/el-dinero-virtual/.

Mobile, JQuery. 2014. JQuery Mobile. JQuery Mobile. [En línea] Fundacion JQuery, 2014. [Citado el: 23 de marzo de 2014.] http://jquerymobile.com/gbs/1.4/.

Nakamoto, Satoshi. 2009. El Bitcoin. Bitcoin. [En línea] 2009. [Citado el: 6 de Julio de 2012.] www.Bitcoin.org/bitcoin.pdf.

Navarro, Javier. 2011. El blog salman. [En línea] 21 de junio de 2011. [Citado el: 24 de octubre de 2012.] http://www.elblogsalmon.com/mercados-financieros/comienzan-las-monedas-virtuales-bitcoin.

Opensource. opensource. [En línea] [Citado el: 28 de octubre de 2013.] http://opensource.org/licenses/mit-license.php.

Pressman. 2002. Ingeniería de software: Un enfoque practico. Roger S. Pressman: s.n., 2002.

Pressman, Roger S. 2002. Ingeniería del software. Madrid : McGraw Hill, 2002.

Quispe, Aline. 2012. De 51. 708 empresas registradas en Bolivia solo 3% son grandes . La Razon. Fin de semana, 2012.

Rogojanu, Angela y Badea, Liana. 2014. The issue of competing currencies Case study-Bitcoin. s.l.: Theoretical and Applied Economics, 2014. págs. 103-114.

Software, Ingenieria de. 2013. Ingenieria de software.mex. *Ingenieria de software.* [En línea] 2013. [Citado el: 24 de octubre de 2013.] http://ingenieriadesoftware.mex.tl/52753_XP---Extreme-Programing.html.

Soto, Jesús Huerta de. 2008. *Dinero, crédito bancario y ciclos ecónomicos.* Madrid : Unión Editorial, 2008. 978-84-7209-473-4.

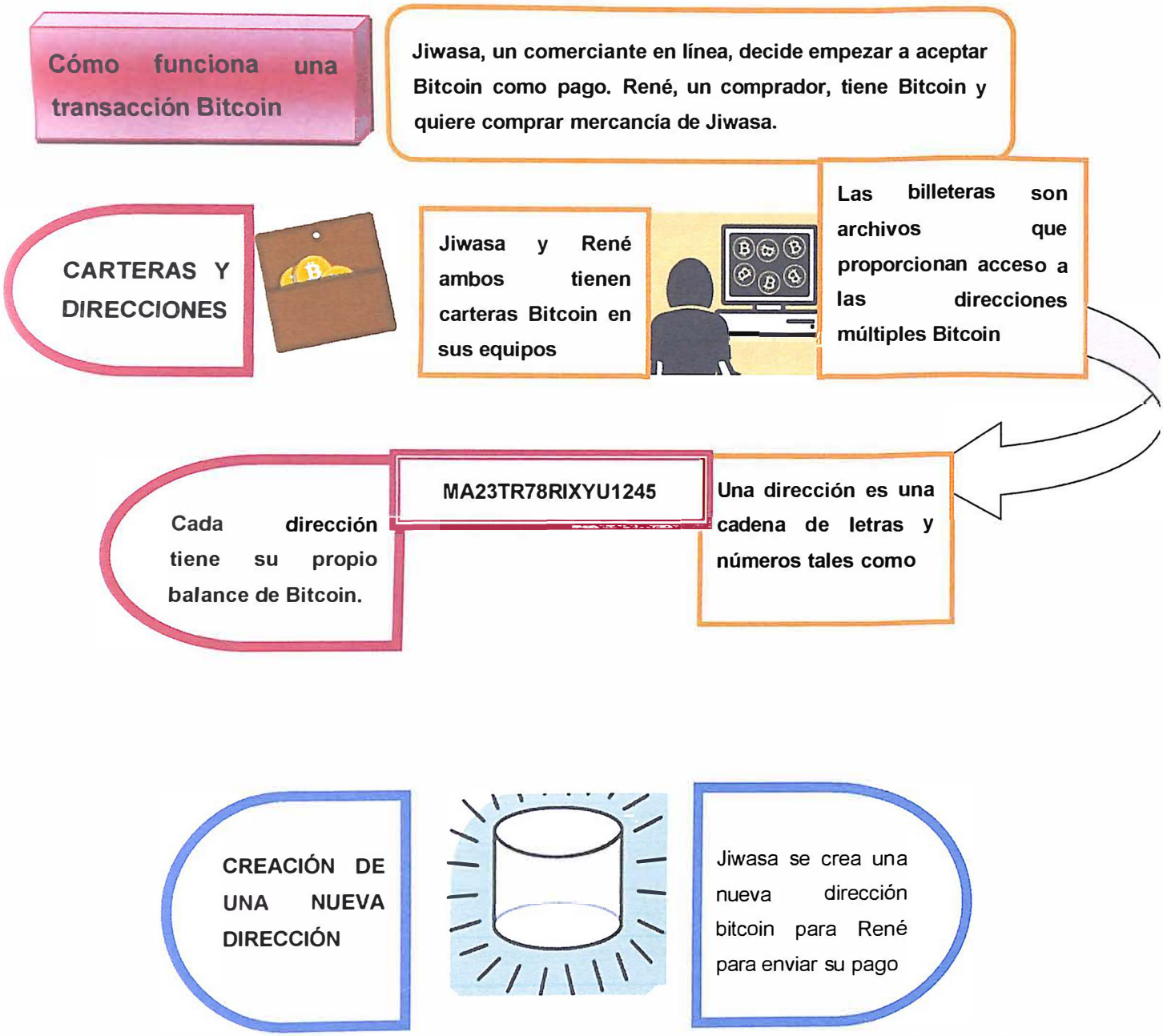
Triana, Miguel. 2011. Miguel Triana. *emtg.* [En línea] 24 de abril de 2011. [Citado el: 26 de agosto de 2013.] http://www.emtg.net78.net/2011/04/24/intro_android.html.

Weatherford, Jack. 1997. *La historia del dinero: De la piedra arenisca al ciberespacio.* Santiago de Chile : Andres Bello, 1997. págs. 57-58-67-157. ISBN 84-89691-45-2.

Weijland, Jan A. Bergstra & Peter. 2014. *Bitcoin: a Money-like Informational Commodity.* Amsterdam : arXiv, 2014.

7. ANEXO

7.1. Funcionamiento de una transacción con Bitcoin

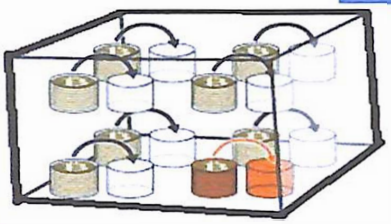


VERIFICACIÓN DE LA TRANSACCIÓN

Tres muchachos son los mineros bitcoin

Su equipo agrupa las transacciones de los últimos 10 minutos en un "bloque de nueva transacción "

Los equipos mineros están preparados para el cálculo de cifrado de funciones gráficas hash

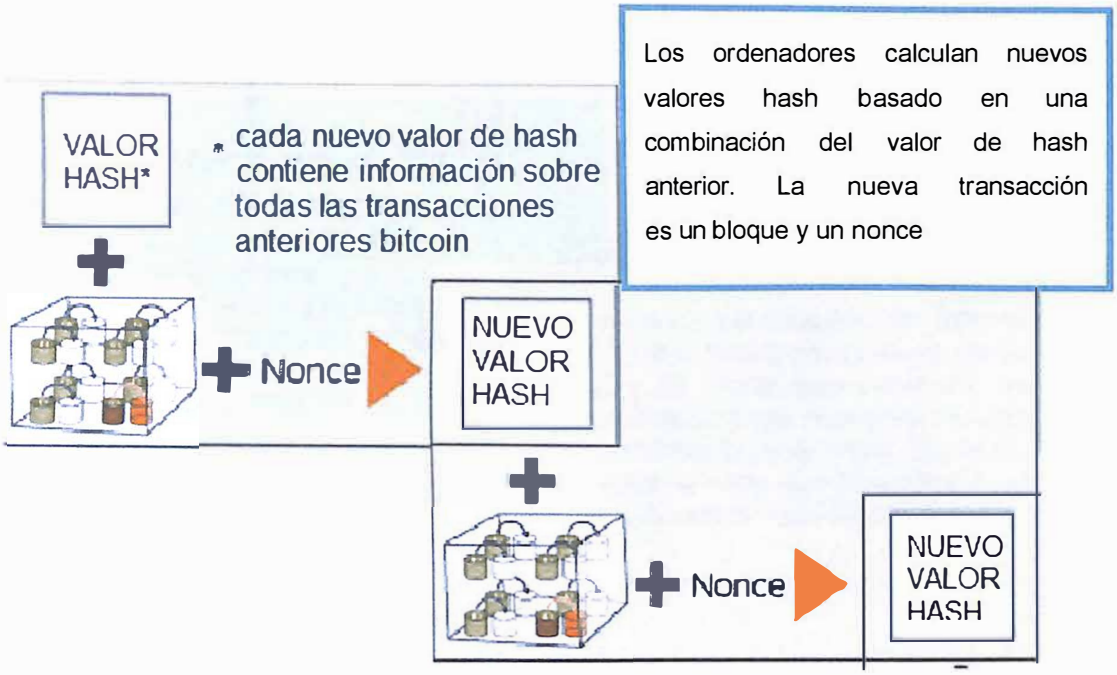


Hashes cryptographic

Las funciones de hash cryptographic es transformar una recopilación de información de datos de una cadena alfanumérica con una longitud fija llamada valor hash. Incluso un cambio pequeño del valor hash resultante y su esencia es imposible predecir qué conjunto de datos inicial va a crear un valor hash específico.

Nonces

Para crear diferentes valores hash de los mismos datos. bitcon utiliza "nonces". Un nonce es un número aleatorio que se añade a los datos antes del hash cambiando los resultados nonce en un valor hash violentamente Diferente



Crear valores hash es computacionalmente trivial, pero el sistema bitcoin requiere que el formulario nuevo hash - específicamente, debe comenzar con un cierto número de ceros

Los mineros no tienen ninguna manera de predecir qué nonce producirá un hash

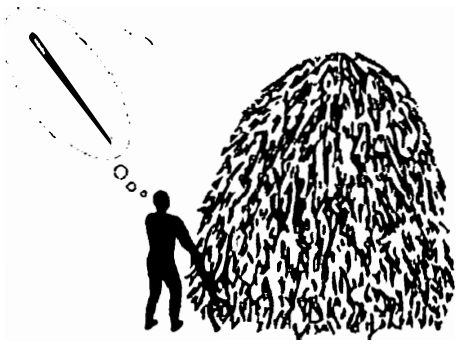
Valor con el número requerido de ceros. por lo que están obligados a generar hashes con muchos nonces diferentes hasta que se produzcan sobre la que trabaja

La criptografía de clave pública 101

Cuando bod crea una nueva dirección lo que realmente está haciendo es generar un "par de claves criptográfico". compuesta de una clave privada y una clave pública. si usted firma un mensaje con una clave privada (que sólo usted sabe). se puede verificar mediante el uso de la clave pública correspondiente (que se sabe que cualquiera) Nueva dirección de Bob bitcoin representa una clave pública única. y la clave privada correspondiente se almacena en su cartera. La clave pública permite a cualquier persona para verificar que un mensaje firmado con la clave privada es válido.

poco diferente.los usuarios de Bitcoin pueden crear tantas direcciones como lo deseen y, de hecho, se les anima a crear uno nuevo para cada nueva transacción para aumentar la privacidad. Siempre y cuando no se sabe qué direcciones son las de Alice, su anonimato se mantiene

Cada bloque incluye un "coinbase" transacción que paga 50 Bitcoin a la ganadora de la minera-en este caso, Gary. una nueva dirección se crea en la cartera de Gary con un saldo de nuevo Bitcoin

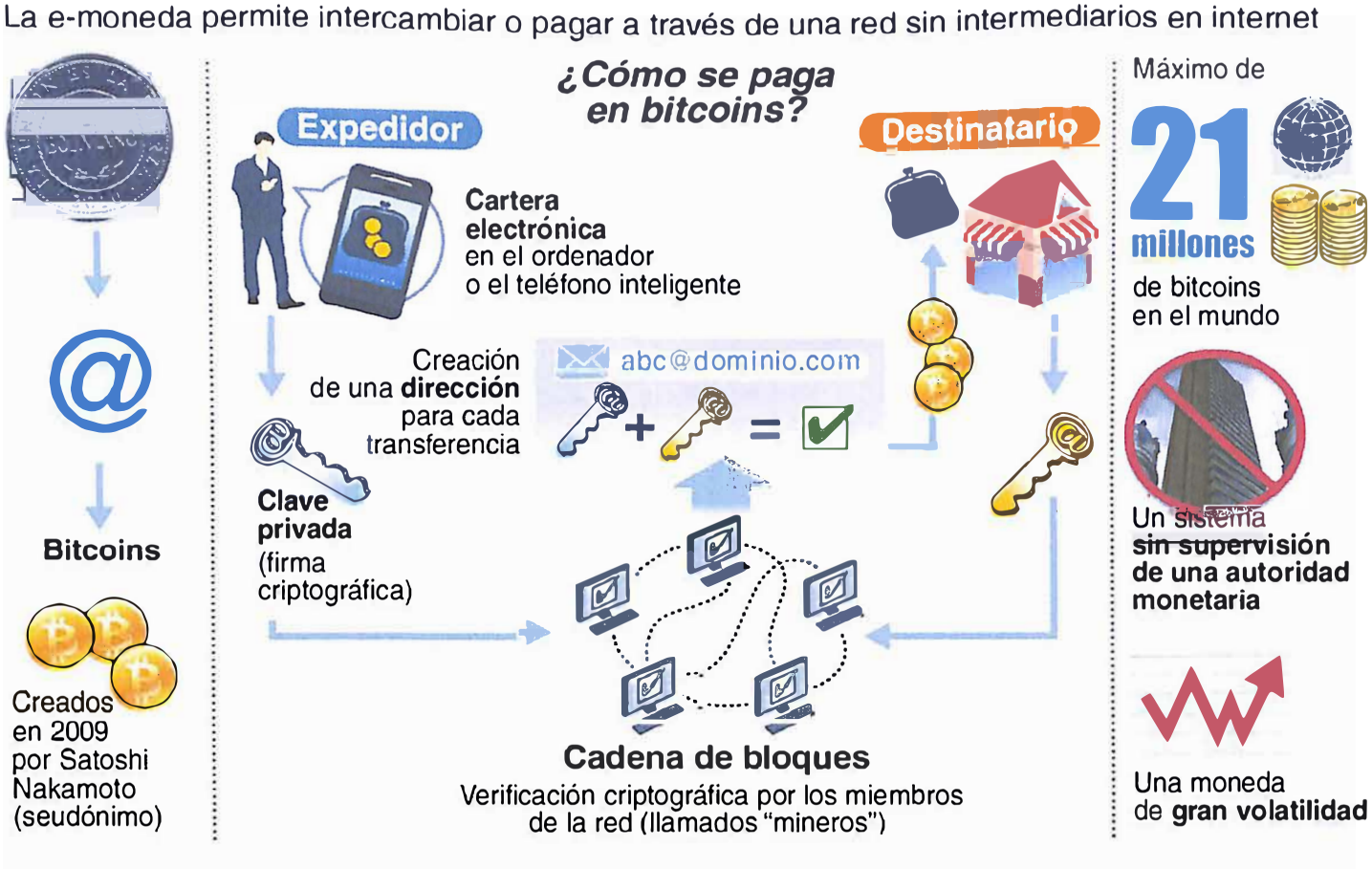


TRANSACCIONES VERIFICADAS

Al paso del tiempo. La transferencia de René a Jiwasa, es sepultados bajo otra transacción más reciente. Además para modificar los detalles, tendría que volver a hacer el trabajo que Gary hizo - porque cualquier cambio requiere un nonce ganador completamente diferente y rehacer el trabajo de los mineros posteriores. Tal hazaña es casi imposible.

Fuente: Elaboración propia.

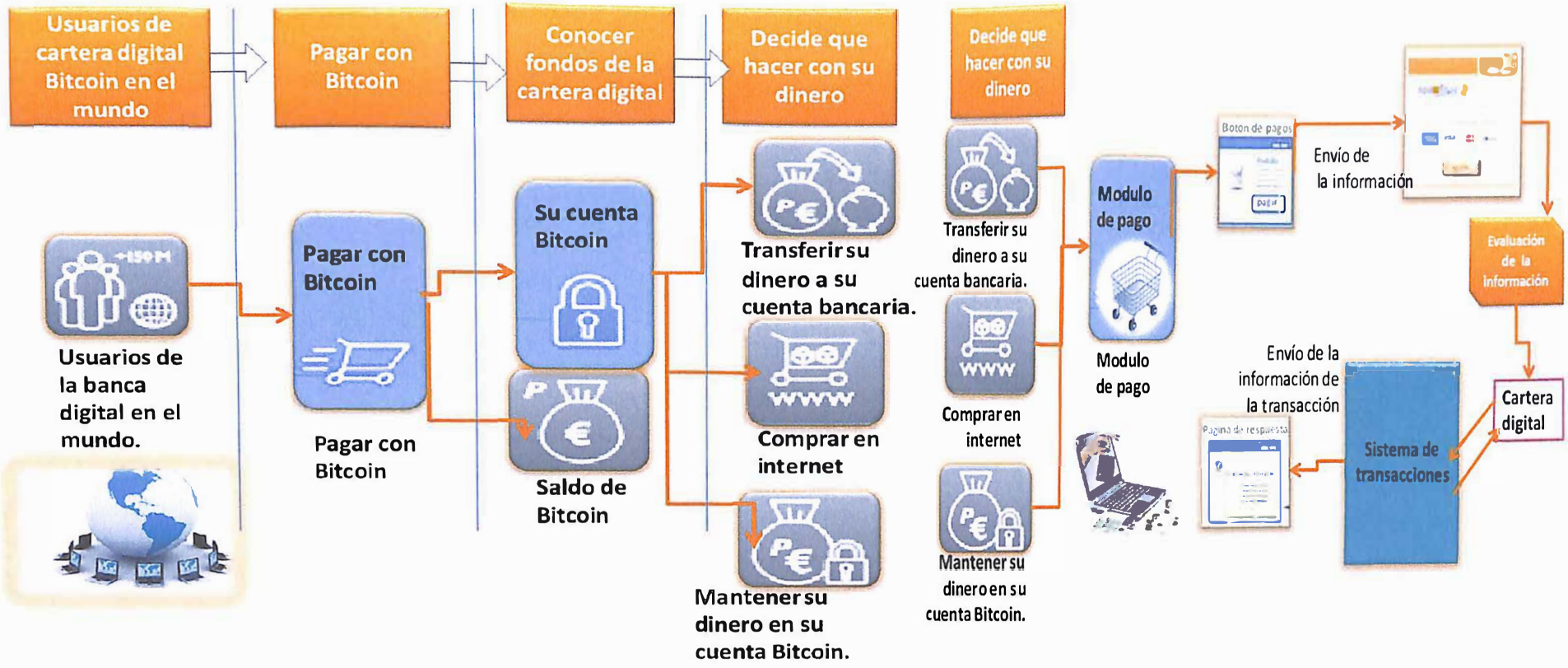
7.2. Esquema de funcionamiento de pago Bitcoin



Fuente: Agencia AFP muestra las características del Bitcoin.

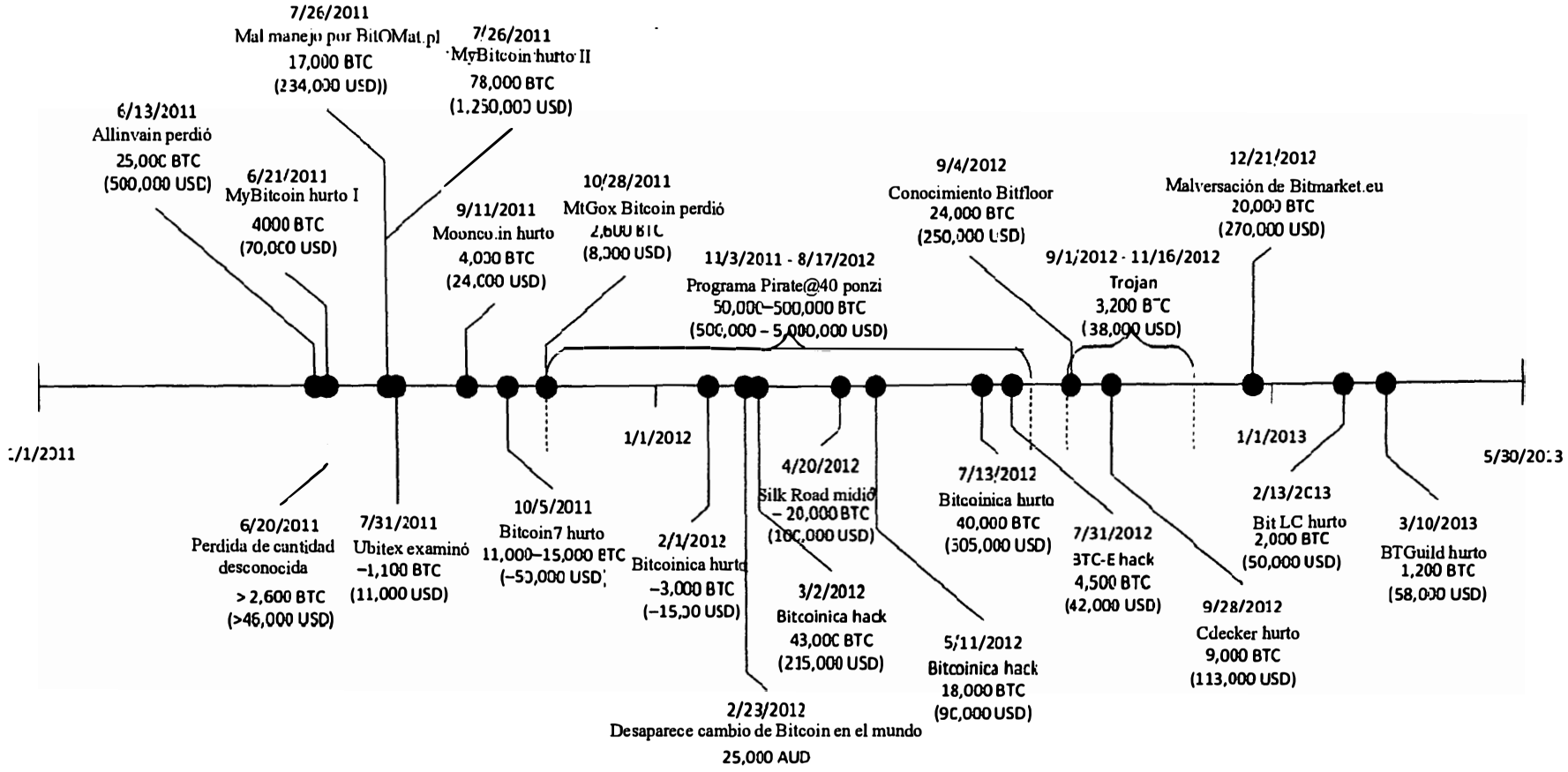
7.3. Esquema de funcionamiento Bitboli

Figura 51: Esquema de funcionamiento del sistema de gestión de moneda digital Bitcoin

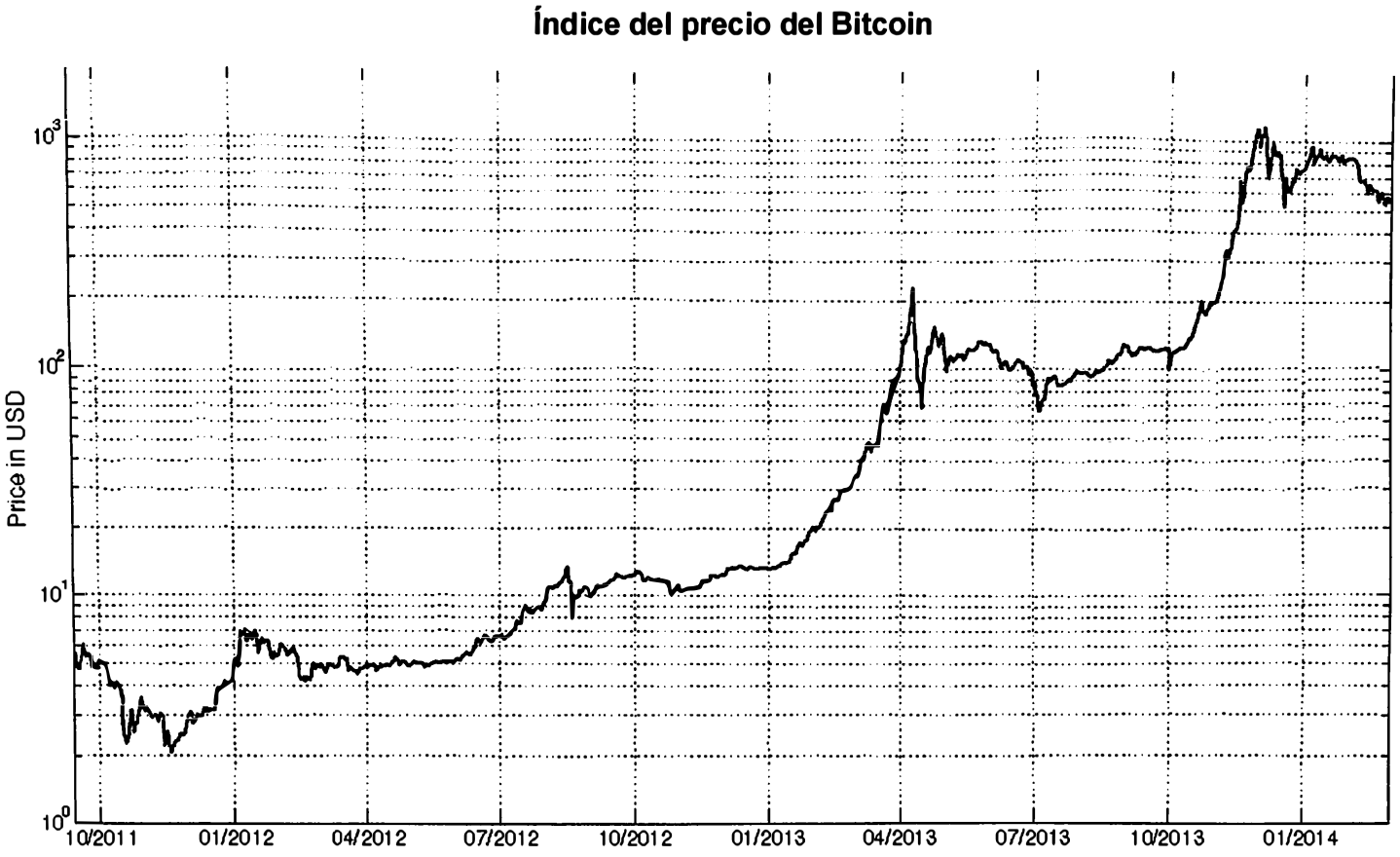


Fuente: Elaboración propia

7.4. Resumen de la evolución del Bitcoin (Krohn, y otros, 2012)



7.5. **Crecimiento de la economía Bitcoin** (Kristoufek, 2014)



7.6. Árbol de problemas

7.7. Marco lógico

	RESUMEN NARRATIVO	INDICADORES OBJETIVAMENTE VARIABLES	MEDIO DE VERIFICACIÓN	SUPUESTOS
FIN	Acceso al mercado bitcoin global de los microempresarios	X % de la población implicada en la compra y venta de los microempresarios satisfechos al momento de usar el sistema durante el primer mes de implementación.	Encuesta sencilla a clientes que usaron dicho sistema y opinión del docente a cargo del tema.	Cliente capacitado y predispuesto para usar el sistema de moneda virtual. Y no hay prohibiciones explícitas por los Estados.
PROPOSITO	Expandir el uso de la moneda digital bitcoin.	X % de expansión de la moneda BTC durante un semestre.	Encuesta a personas al azar, preguntando el conocimiento hacia la moneda.	Sistema operativo listo para actuar como cartera móvil con la moneda digital bitcoin.
PRODUCTO	Sistema de gestión basada en la web que permita realizar transacciones con la moneda bitcoin de una cuenta a otra.	Una aplicación móvil que: Permita realizar transacciones con bitcoin, permita monitorear la información con respecto al constante cambio del valor del BTC. Elaborada hasta 2014.	HTML5 – PhoneGap - JavaScript (diseño) UML - Entidad relación - MySQL - Minero de bitcoin 0-6.3	Software instalado en el hardware del cliente con acceso a internet.
ACTIVIDADES	Revisar documentación acerca de:Comercio con moneda virtual - revisar el código abierto del bitcoin - diseñar el modelo UML para el desarrollo del software - desarrollar el módulo de manejo de cuentas.	Diagrama de Gantt: Página 101 diagrama de Gantt.	Verificación del docente a cargo de la revisión en cada actividad, culminada.	Tener el código necesario para la modificación y elaboración del módulo de manejo de cuentas.

Cerámicas Jiwasa

El Alto, 25 de Julio de 2014

CARTA DE CONFORMIDAD

Sr. Ing.
Walter Carvajal
Coordinador de carrera en Ingeniería de sistemas
UNIVERSIDAD LA SALLE BOLIVIA

De mi consideración:

Por la presente yo Elizardo Melendrez Calle en calidad de Gerente General de CERAMICAS JIWASA, certifico que la señorita Gabriela Melendrez Alaro ha realizado el proyecto "CARTERA MÓVIL DIGITAL DE DINERO VIRTUAL BITCOIN PARA MICROEMPRESAS BOLIVIANAS", desarrollado para nuestra microempresa conforme a las características propuestas para la ejecución del proyecto. Cumpliendo satisfactoriamente con los objetivos planteados.

Atentamente:

Elizardo Melendrez C.
GERENTE PROPIETARIO
CERAMICAS JIWASA

Elizardo Melendrez Calle
CERAMICAS JIWASA

Avenida # 192 Zona San Agustin ciudad de El Alto Cel. 72513195, E mail.
ceramicasjiwasa@hotmail.com