ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ANÁLISIS DE LA UTILIZACIÓN DE LA TECNOLOGÍA BLOCKCHAIN PARA LA GESTIÓN DE LA INFORMACIÓN EN SISTEMAS DE ALARMAS RESIDENCIALES

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

ALEXANDRA KARINA CARRIÓN BASANTES

alexita_blue@yahoo.es

DIRECTOR: Dr. DIEGO REINOSO

diego.reinoso@epn.edu.ec

CODIRECTOR: Ing. JORGE CARVAJAL, MSc.

jorge.carvajal@epn.edu.ec

Quito, septiembre 2018

AVAL

Certificamos que el presente trabajo fue desarrollado por Alexandra Karina Carrión Basantes, bajo nuestra supervisión.

Dr. DIEGO REINOSO
DIRECTOR DEL TRABAJO DE TITULACIÓN

Ing. JORGE CARVAJAL, MSc.
CODIRECTOR DEL TRABAJO DE TITULACIÓN

DECLARACIÓN DE AUTORÍA

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

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la Normatividad Institucional Vigente.

Alexandra Karina Carrión Basantes

DEDICATORIA

El presente estudio está dedicado para la persona más importante de mi vida, mi quería y amada madre, Paty. Su incondicional amor y sabiduría han sido mi motivación para lograr esta meta. Sin ti, este sueño no hubiera sido posible, así que, este triunfo también es tuyo.

Además, dedicó este trabajo a todas las personas soñadoras que luchan cada día por contribuir con ideas innovadoras para crear nuevos productos con un valor agregado que proporcione mayor competitividad a nuestra sociedad más allá del mercado local por medio de un esquema eficiente y seguro.

AGRADECIMIENTO

En primer lugar, agradezco a Dios por ser mi compañía, guía y cuidarme durante toda mi vida. Gracias por darme una hermosa familia, brindarme sabiduría, perseverancia y fortaleza para culminar mis metas.

A mi amiga y compañera de todos los días, mi querida madre Paty, gracias por toda tu paciencia y por el amor infinito que me das siempre. Por enseñarme a luchar y no abandonar mis sueños. Por tus consejos y palabras de aliento en esos días grises. Sin ti no sería quien soy actualmente.

A mis hermanos David, Edy, Santy y Diany, por ser un pilar fundamental en mi vida. Gracias por darme ánimo para terminar este trabajo. Durante este tiempo, me han enseñado a hacer las cosas con amor y de la mejor manera.

Mi gratitud a Daniel, por acompañarme en esta etapa tan importante de mi vida. Tus experiencias y consejos han brindado un aporte significativo a este estudio.

También quiero agradecer a mi director Diego Reinoso y codirector de tesis Jorge Carvajal, por su dirección, colaboración y recomendaciones. Gracias por dedicar parte de su tiempo para revisar, corregir y aportar con valiosas ideas en la realización de este trabajo.

ÍNDICE DE CONTENIDO

RESUMEN

El presente proyecto propone el análisis de la utilización de la Tecnología *Blockchain* “Cadena de Bloques” para la gestión de la información en sistemas de alarmas residenciales tomando en cuenta la plataforma descentralizada *Ethereum*, sin la necesidad de contratar a un intermediario para la prestación de este servicio.

La gestión y adquisición de la información ha evolucionado de acuerdo a la influencia de los avances tecnológicos, el desarrollo de los sistemas descentralizados y contratos inteligentes, han mejorado las ineficiencias de los actuales servicios centralizados.

La fase teórica describirá brevemente las características y conceptos fundamentales de la cadena de bloques, su estructura, arquitectura, topología, algoritmo de consenso, plataformas y algunas aplicaciones descentralizadas en la red *peer-to-peer*.

Se analizará cuál ha sido la evolución y crecimiento de los sistemas de alarmas residenciales. Se realizará un estudio de los sistemas de alarmas residenciales de 30 casas que podrían contar con el nuevo sistema de seguridad tomando en cuenta los principios de la *Blockchain* privada.

En la fase del análisis de la gestión de los eventos, se presentará un cuadro comparativo de ventajas y desventajas del sistema de alarmas centralizado convencional y el nuevo sistema de seguridad descentralizado basado en la tecnología *Blockchain*. No se diseñará, ni implementará ningún prototipo; en cambio, se mostrará la simulación de la red *peer-to-peer* considerando la plataforma *Ethereum* basada en el estándar dado por el *token* ERC20.

En la etapa del análisis de costos, se describirá el coste de equipos, accesorios, monitoreo, instalación y mantenimiento que necesitará el sistema de alarmas centralizado y descentralizado.

Finalmente, se mencionarán las conclusiones y recomendaciones de este estudio técnico, que pretende contribuir para futuras investigaciones con respecto a los sistemas descentralizados.

PALABRAS CLAVE: aplicaciones descentralizadas, *Blockchain* privada, contratos inteligentes, plataforma *Ethereum*, red *peer-to-peer*, sistemas descentralizados, tecnología *Blockchain* y *token* ERC20.

ABSTRACT

This project proposes the analysis of the use of Blockchain Technology for the management of information in residential alarm systems taking into account the decentralized platform Ethereum, without the need of hiring an intermediary for the provision of this service.

The management and acquisition of information has evolved drastically through the influence of new technological advances, the development of decentralized systems and smart contracts. These innovations have improved the inefficiencies of the current centralized services.

The theoretical phase will briefly describe the main characteristics and concepts of the Blockchain: structure, architecture, topology, consensus algorithm, platforms and some decentralized applications through the peer-to-peer network.

The evolution and growth of residential alarm systems will be analyzed. A study will be made of the residential alarm systems of 30 houses that could have the new security system, taking into account, the principles of the private Blockchain.

In the management analysis of the events, a comparative chart of the advantages and disadvantages of the conventional centralized alarm system and the new decentralized security system based on the Blockchain technology will be presented. The design or implementation of a prototype is not included as part of this project, instead the peer-to-peer network simulation will be shown, considering the Ethereum platform based on the standard given by the ERC20 token.

In the cost analysis stage, the cost of equipment, accessories, monitoring, installation and maintenance that would be necessary for the centralized and decentralized alarm system will be described.

Finally, the conclusions and recommendations of this technical study will be mentioned, which intends to contribute to future research with respect to decentralized systems.

KEYWORDS: Blockchain technology**,** decentralized applications**,** decentralized systems**,** Ethereum platform**,** peer-to-peer network**,** private Blockchain**,** smart contracts and token ERC20.

1. INTRODUCCIÓN

En la sociedad del conocimiento y la información, la comunicación ha ido evolucionando gracias a los avances tecnológicos. La cadena de bloques o *Blockchain* ha surgido durante esta década generando un sinnúmero de oportunidades en el mercado digital a nivel mundial. Este paradigma tecnológico ha revolucionado los sistemas digitales de forma eficiente y automática a través de un modelo descentralizado dentro de la red *peer-to-peer*.

Desde el nacimiento de esta nueva tecnología, no han dejado de crecer las aplicaciones, por ejemplo, se ha incursionado en nuevos modelos de negocios, se ha eliminado la dependencia de la concentración de recursos que se presenta en los esquemas centralizados. De esta manera, *Blockchain* se convierte en una herramienta poderosa para las comunicaciones de forma más rápida y segura. Aumenta la competitividad del servicio, facilitando la migración de información a un modelo descentralizado de forma transparente, óptima y confiable.

Actualmente, *Blockchain* ha incursionado en los sistemas de comunicaciones a nivel mundial en combinación con otras tecnologías como el Internet de las Cosas (*IoT*), *BigData,* 5G, inteligencia artificial, entre otras. Pero, al ser una tecnología muy joven, aún necesita incursionar en otros campos, como, el sector de Telecomunicaciones. En el presente estudio se realizará un análisis de la utilización de la tecnología *Blockchain* para la gestión de la información en sistemas de alarmas residenciales.

Durante mucho tiempo, los sistemas de alarmas han tenido un enfoque centralizado. El principal problema radica en los datos, que convergen en un solo sitio. La estación de monitoreo presenta un retardo en el tiempo de respuesta, por no contar con una ubicación estratégica ante una emergencia al domicilio o cooperar con la UPC. Este inconveniente, multiplicado por el número de usuarios residenciales conlleva un gasto aún mayor.

La idea es aprovechar el potencial que brinda la tecnología *Blockchain*, con sus datos distribuidos y almacenados de una forma automática, optimizando sus recursos, sin la necesidad de intermediarios. La integración de la comunidad mediante el consenso de eventos incentiva a los propios miembros a cooperar en su seguridad.

En este trabajo, se analizará la cadena de bloques con relación a las alarmas residenciales donde los usuarios contarán con un registro público, participarán en la toma de decisión y estarán informados de las transacciones generadas. Esto implica que la gestión de información será descentralizada sobre Internet, sin necesidad de contratar a un intermediario para el monitoreo.

1.1 Objetivos

Objetivo general

Realizar un análisis de la utilización de la Tecnología *Blockchain* para la gestión de información en sistemas de alarmas residenciales.

Objetivos específicos

- Describir los conceptos fundamentos y características generales de la Tecnología *Blockchain*.
- Identificar los beneficios de la Tecnología *Blockchain* en el sector de telecomunicaciones.
- Analizar la situación actual del sistema de alarmas en los hogares.
- Realizar un análisis comparativo del sistema de alarmas residenciales y la utilización de la nueva tecnología *Blockchain* para la gestión de la información.

1.2 Alcance

Este trabajo de titulación realizará sólo un estudio de las características y fundamentos de la nueva Tecnología *Blockchain*, basándose en el sistema descentralizado y en el algoritmo de consenso entre los nodos de la red P2P y sus aplicaciones en el sector de telecomunicaciones.

Al estudiar esta nueva tecnología se pretende revolucionar la forma de gestión de la información, reduciendo los riesgos de errores humanos al depender de intermediarios. Además, desde el nacimiento de esta nueva Tecnología no ha dejado de crecer las aplicaciones en diferentes sectores, convirtiéndose en una herramienta poderosa para las comunicaciones de forma más rápida y barata.

Al ser el primer estudio realizado sobre este tema en la carrera, se analizará las ventajas en la gestión de los eventos teniendo en cuenta la plataforma distribuida *Ethereum* con una estructura descentralizada. Por lo tanto, la implementación de un prototipo esta fuera del alcance del proyecto.

Se realizará un análisis de la situación del estado actual de los sistemas de alarmas en hogares, mediante un sistema centralizado y la contratación de una empresa para el monitoreo y seguridad. Posteriormente se realizará el análisis de costos.

Se utilizarán los principios básicos de la tecnología de Cadena de Bloques para la gestión de la información en los sistemas de alarmas residenciales, mediante la confiabilidad y seguridad de los datos entre los usuarios que pertenecen a la red peer-to-peer, sin necesidad de intermediarios, a través de Internet. Se realizará el análisis de costos de los mismos.

Finalmente, en este trabajo se realizará un análisis sobre la utilización de la Tecnología *Blockchain* en virtud de las ventajas y el coste.

1.3 Marco Teórico

1.3.1 Sistema de alarma residencial tradicional

Un sistema de alarma residencial convencional o también conocido como sistema de seguridad contra intrusión consiste en un conjunto de equipos electrónicos y sensores. Comúnmente, estos dispositivos se localizan en ciertos puntos y áreas estratégicas de la residencia o conjunto habitacional. Su principal objetivo es prevenir o neutralizar una situación de peligro y reportar al usuario los eventos de alerta que se generan.

Estos sistemas prestan especial énfasis en la supervisión y monitoreo del equipamiento de seguridad. Al mismo tiempo, atenúa el sentimiento de incomodidad al dejar deshabitada la residencia o establecimiento. Los sistemas de alarma proporcionan eventos desfavorables o fallas cuando se genera alguna situación anormal dentro del área de acción y garantizan su protección. Por lo tanto, representan un beneficio subyacente en la instalación. Además, permite a las personas mejorar su situación emocional y proteger su entorno familiar.

Evolución y crecimiento del sistema de alarmas residencial

Los sistemas de alarmas residenciales han evolucionado en función del avance tecnológico y los requerimientos de los clientes. Este desarrollo incluye al hardware (dispositivos y sensores de alarma), software (manejo de la base de datos del usuario) y monitoreo de los eventos (comunicación con el personal de seguridad o policía). A continuación, se menciona las etapas de la evolución y crecimiento de los sistemas de alarmas convencionales.

Al principio, los sistemas de alarmas residenciales sólo contaban con un dispositivo sonoro que indicaba la presencia de una intrusión. El usuario era el encargado de controlar manualmente los eventos para el funcionamiento de la alarma. El principal problema se generó al producirse muchas falsas alarmas [1].

Luego se presenta un esquema centralizado donde se disminuyen los errores de falsos eventos, pero ahora el problema se presentó en la recopilación de la información de forma analógica. Las grabaciones se almacenaban en cintas de video, lo que provocó que con el tiempo llegaran a ocupar gran espacio o incluso en ciertas ocasiones se dañaban y se perdía toda la información de respaldo.

En vista del desarrollo tecnológico se implementaron dispositivos electrónicos para monitorear los eventos remotamente. Como resultado, se facilitó su integración con otros sistemas, con la posibilidad de almacenar las imágenes digitalmente. En este caso, la información aún depende de la central de control y los eventos que se generan son monitorizados por un operador. La empresa se encarga de contactarse con el personal de seguridad y frente a alguna alerta se genera una alarma por sonido, texto o imagen [2].

La siguiente fase considera que los sistemas de seguridad contra intrusión han evolucionado de acuerdo a los requerimientos del usuario. Con un menor tiempo de respuesta, mayor confiabilidad, un mínimo de fallo y con un equipamiento de última tecnología. Es así, que se pueden complementar los sistemas de alarmas residenciales con CCTV[1], cámaras que graben en tiempo real y automáticamente cualquier acto delictivo en el panel de alarmas. Esto implica para el cliente un mayor costo por este servicio.

Componentes y características del sistema de alarmas

La característica de los sistemas de alarmas se presenta en la integración de elementos y dispositivos electrónicos que se conectan al panel de alarmas y desde éste hacia la central receptora de alarmas (CRA). Los detectores de alarma se conectan en un circuito cerrado y se distribuyen por zonas, para que su activación o desactivación sea de forma rápida y de acuerdo a su ubicación.

La figura 1.1 indica un circuito simple compuesto por el panel de alarma, sensores y sirena. A continuación, se detallan los elementos principales de ese sistema de alarmas:

- Panel de alarma.- Constituye el circuito electrónico donde se conectan los sensores (dispositivos de entrada), módulos (dispositivos de salida), transformador, batería, teclado y sirena. La figura 1.1 muestra el panel PC1832, que trabaja con 8 zonas y 2 salidas programables, PGM1 y PGM2. El panel controla el continuo funcionamiento de los dispositivos y zonas.

[1]CCTV (*Closed Circuit Television*): Circuito cerrado de televisión, donde todos los componentes del sistema están conectados unos con otros, por lo general están formados por un conjunto de cámaras y monitores ubicados en una sala central.

Figura 1.1 Conexión del panel de alarma PC1832 y sensores.

- Sensores.- Son los elementos cableados o inalámbricos, como el contacto magnético e infrarrojo. Permiten vigilar los accesos de la vivienda dentro de un lugar determinado. Si se opta por un sistema cableado, los sensores necesitan de una alimentación paralela para su funcionamiento.
- Sirena.- Es el dispositivo acústico, que emite señales sonoras al existir una variación en los sensores. Sirve para asustar al intruso, incluso antes que entre o cause algún daño en la vivienda.
- Transformador.- Dispositivo que transforma los 220V a 16.5V, proporciona la energía eléctrica para el panel, elementos y batería.
- Batería.- Este elemento entra en funcionamiento en caso de fallas eléctricas, proporciona autonomía y trabajo continúo al sistema. En las instalaciones residenciales contra hurto, brinda una alimentación de *standby* de 4 horas.
- Teclado.- Es el dispositivo de entrada, de fácil acceso para configurar, activar o desactivar las funciones del sistema [3].

Cuando se produce una falsa alarma, el usuario puede desactivar la alarma pulsando la clave de 4 dígitos, que es asignada por el proveedor del servicio. Los datos de los eventos se registran automáticamente en la base de datos de un ordenador central por parte de la operadora que brinda el monitoreo las 24 horas del día. En general, los sistemas de alarmas varían en función de las necesidades del usuario, presupuesto, infraestructura y características técnicas.

Equipamiento puertas adentro

El principal componente de equipamiento que tiene cada usuario en sus hogares es el panel de alarmas. Su función primordial es monitorear los sensores y señales de robo, incendio o pánico que fueran detectadas. Este equipo comunica todos los eventos a una central de monitoreo que está ubicada en la oficina de la empresa proveedora de este servicio.

La figura 1.2 presenta el panel de alarmas más común en el mercado local. Contiene una tarjeta electrónica que recibe la información de los sensores ya sean contactos magnéticos, sensores de movimiento o detectores de humo. Los sensores de movimiento en puertas o ventanas, detectores de humo, sensor de ruptura de vidrios, infrarrojos, por mencionar algunos ejemplos. Estos dispositivos son instalados según la norma NFPA 72 y el estándar de paneles de control ANSI/SIA CP-01-2000 [4].

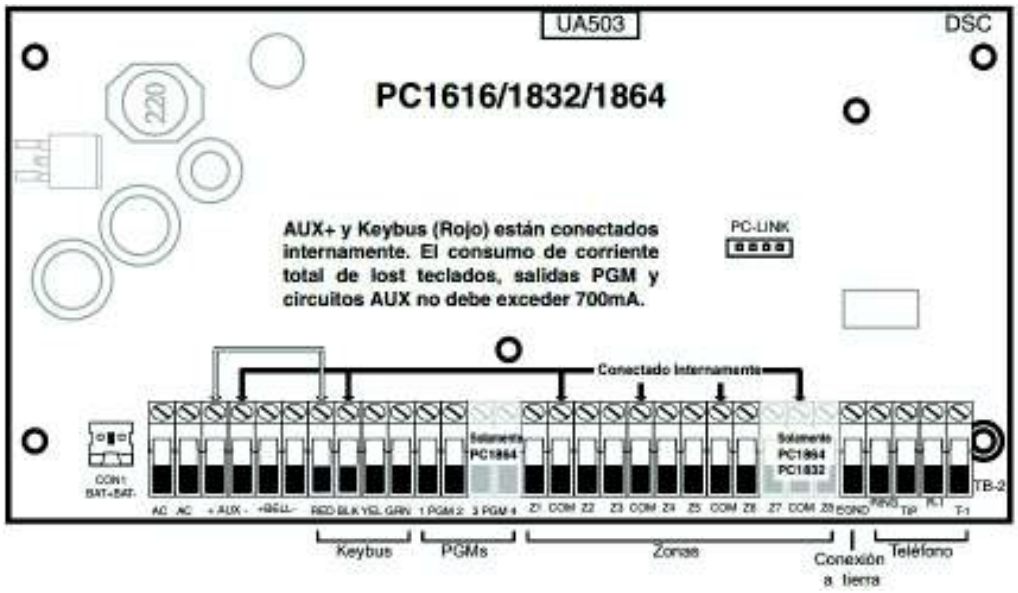

Figura 1.2 Panel de Alarmas [5].

Adicionalmente, la tarjeta electrónica dispone de puertos para conectar una sirena u otro dispositivo mediante salidas programables. Opcionalmente, estas salidas pueden ser usadas para accionar luces estroboscópicas, sirenas, cerraduras magnéticas, etc. Todo el sistema es configurado y controlado mediante un teclado alfanumérico; el teclado facilita la configuración del panel así también como para “armar” o “desarmar” el sistema; cabe mencionar brevemente que estos términos refieren al cambio de disposición, dejando el equipo listo para ejecutar las salidas y notificar alarmas dependiendo del estado de los sensores, complementariamente se requiere fuentes de energía con respaldo de batería.

Gestión de eventos, control y seguridad del sistema de alarmas

El equipamiento instalado en los hogares puede reportar ciertos eventos cuando el lugar este bajo alarma, el reporte lo recibe directamente la central de monitoreo comercial. Por lo general, el control de los eventos desde la central es mediante las líneas telefónicas convencionales. Estas siguen siendo hoy en día la principal forma de comunicar eventos utilizando tonos DTMF[2].

La transmisión se produce por una llamada telefónica, se bloquea el teléfono cuando un evento ocurre, es decir, el panel toma posesión de la línea e interrumpe cualquier llamada en proceso, para dar prioridad a la señal codificada, donde la central recibe y decodifica la señal ya sea por la transmisión de los códigos DTMF correspondientes al evento.

La figura 1.3 muestra la conexión de la línea telefónica a los terminales de retorno y *Tip and Ring* del panel, similares a los de un teléfono analógico. El número de veces que intentará realizar una llamada y los números de teléfono de la central de monitoreo son campos configurables mediante el teclado del panel.

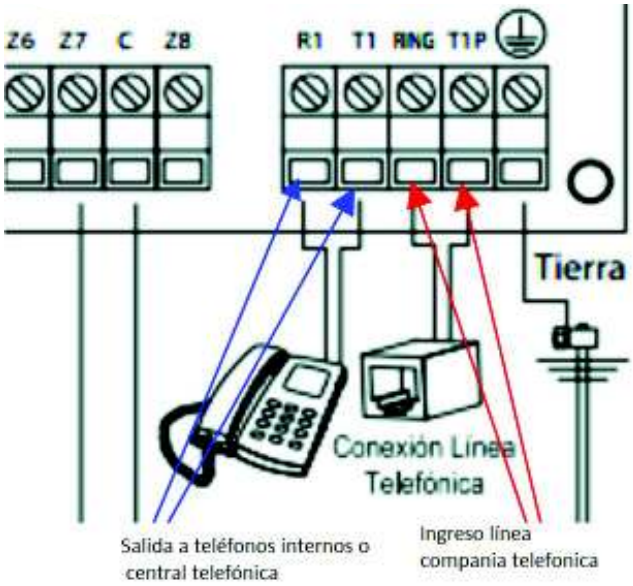

Figura 1.3 Conexión de la línea telefónica en el panel [6]

El medio de transmisión puede cambiar, sin embargo, la información es siempre centralizada. De hecho, las centrales de monitoreo modernas como las Sur-Gard *System,* cuentan con varios puertos de comunicación Ethernet para recibir la información de los paneles de alarmas utilizando protocolos TCP-IP [7].

[2] DTMF (*Dual-Tone MultiFrequency*): Mezcla matricial de dos tonos en algún estándar propio del panel y la central, generalmente Contact ID

Por lo habitual, la programación de un número telefónico se incluye en el panel de alarma y son registrados en la central. Este modelo por su carácter centralizado maneja un gran número de troncales para recibir todas las llamadas telefónicas entrantes desde cualquier línea proveniente de cada uno de los paneles de alarma registrados en los hogares.

El formato de comunicación a través de la línea telefónica depende de las características del panel disponible en la casa de cada usuario, como por ejemplo, Contact ID[3], Acron[4], Scantronics[5]. Por lo tanto, el formato más común dado por el estándar *Security Industry Standards*, SIA, es el Contact ID [8].

Las estaciones centrales están ubicadas, por lo general, en las instalaciones de las diferentes empresas de seguridad y monitoreo locales. La seguridad del sistema de alarmas está a cargo de estas empresas que realiza el monitoreo de los eventos a través de la central receptora de alarmas. La CRA se encarga de monitorear las señales de alarma vía teléfono, radio o internet y aplicar el respectivo mecanismo de seguridad ante la activación de un evento de emergencia ya sea con el respaldo del personal de seguridad, policía o bomberos, según el tipo de intrusión.

Por lo tanto, constituye una vía de comunicación directa entre los propietarios de las viviendas y el personal de seguridad o técnico de la empresa. Generalmente, el personal designado para el monitoreo cuenta con una interfaz y maneja una base de datos de todos los usuarios, donde registra un archivo histórico de todos los eventos.

La empresa de monitoreo en todo momento está pendiente de los eventos recibidos desde los paneles de alarma. Si se genera una situación de alarma se encarga de contactar al personal asignado a ese sector o a su vez a la entidad competente previa confirmación de que la alarma no sea falsa. Además, los paneles de alarma indican a la central los problemas de mantenimiento o fallas.

Normalmente, los usuarios pagan mensualmente por el servicio de monitoreo y firman un contrato anual; que contempla la instalación de los equipos de alarma, mantenimiento y control de accesos. Además, las compañías de seguridad se comprometen a brindar eficiencia y calidad en su asistencia.

---

[3] *Contact ID*: Es una secuencia de tonos DTMF, agrupados en determinado orden para que la central de alarmas identifique el evento. El panel de alarmas marca a la central y le informa de los eventos mediante pulsaciones a una frecuencia definida por el estándar.
[4] *Acron*: Formato de comunicación DTMF, permite transmitir 8 dígitos en un slot de tiempo.
[5] *Scantronic:* Trabaja con tonos DTMF para configurar de 8 a 16 zonas, 1 digito para supervisión y con 4 a 6 digitos para accesos de eventos.

Sistema actual de monitoreo comunitario

Las alarmas comunitarias son sistemas de prevención que se activan ante la presencia de una intrusión. Sin embargo, estos son dependientes de la intervención de todos los vecinos de manera organizada. Entonces, estos sistemas son activados directamente por el usuario mediante dispositivos móviles. Actualmente, Quito cuenta con 1.201 sistemas de alarmas comunitarias, instaladas por parte del Municipio desde el 2014.

El objetivo es reducir los niveles de delincuencia. Los principales problemas yacen en la alta demanda de los barrios y los pocos dispositivos, en otros casos, las comunidades no están preparadas para poseer una alarma debido a la falta de trabajo en conjunto. El funcionamiento óptimo de los sistemas comunitarios se presenta cuando los barrios capitalinos se empoderan de su propia seguridad, sobresale el compromiso colectivo, con el respaldo del UPC ha disminuido el robo y atraco [9].

La información de los eventos generados, es centralizada a los diferentes puntos donde se encuentra la administración del sistema como es la Secretaria de Seguridad del Municipio. Si existe una alerta de emergencia se retransmitida al personal de la UPC del sector, quien puede visualizar el sistema de alarma mediante una página web. Cuando una alarma es activada, se emite una señal auditiva para la comunidad y se muestra en un computador de la UPC el mapa del lugar geo referencial y todos los datos del usuario, donde se produce el evento de emergencia. La policía llama al usuario registrado en el sistema y si no encuentra respuesta, acude al sitio a cerrar la alarma y posteriormente realiza un informe de lo ocurrido. El tiempo de reacción de la policía se estima en 5 minutos.

Por ejemplo, en el sector de La Luz, las alarmas comunitarias fueron instaladas hace 4 años y dan servicio a 26 direcciones, incluido el domicilio del administrador del sistema de ese sector. El mantenimiento del sistema se realiza cada 4 meses por parte del municipio. Habitualmente al mes se atiende 2 alertas de alarma comunitaria y el tiempo de respuesta desde la activación es de 3 a 5 minutos, según información recogida de los policías del lugar en el mes de abril 2018. La policía recibe más alertas vía telefónica, por la página web o por el sistema TIA POLI[6].

[6] TIA POLI: Este término hace referencia al servicio del botón de seguridad en los barrios de Quito, que se activa por la marcación rápida de la tecla número 5 del celular.

1.3.2 Tecnología *Blockchain*

Blockchain nace del protocolo Bitcoin[7], en 2008, por Satoshi Nakamoto, seudónimo o alias de una persona o varias personas. Esta tecnología aparece con la finalidad de resolver varios problemas del campo financiero. Entre los que se destacan, la confianza para realizar las transacciones, excesivo cobro en la cuenta bancaria, pago de impuestos por transferencia de dinero y retrasos por intermediarios financieros o bancos centrales [10].

De esta manera, *Blockchain* constituye una tecnología relativamente nueva. Apareció hace pocos años en el mundo digital. Sin embargo, ha causado un boom en varias empresas y organizaciones en países de Europa, Estados Unidos y China. Estos han sido los precursores para impulsar este paradigma que enlazan las comunicaciones tradicionales con esta nueva tecnología.

Blockchain es una tecnología tan prometedora como lo era Internet hace 20 años, así lo pública el diario inglés Financial Times. Además, cuenta con el respaldo de los multimillonarios empresarios Bill Gates y Richard Branson; el gran interés que tiene las compañías IBM, Siemens, Sony y PwC, que cuentan con productos ya patentados. Por lo tanto, los beneficios no solo se centran al ámbito financiero, sino a innumerables campos en especial al sector de las Telecomunicaciones [11].

Dada esta premisa, en base al sector financiero se han hecho mejoras con respecto a la eficiencia del servicio. Al mismo tiempo, esto ha servido para que poco a poco se vayan desarrollando sistemas y aplicaciones inimaginables basadas en esta tecnología; en la industria tecnológica, sanitaria, ciberseguridad, de salud y entretenimiento, así como también se han desarrollado mejoras en los productos y/o servicios.

Por otra parte, la mayor parte de proyectos se encuentran en la plataforma *GitHub*[8], más reconocida de software libre a nivel mundial. Cuenta con más de 28 millones de colaboradores y un repositorio que alberga más de 85 millones de aplicaciones descentralizadas [12]. Este ecosistema sobre Internet maneja estándares comunes, permite a los usuarios tener confiabilidad en el algoritmo y proceso de consenso, contribuir con la programación, copiar la documentación o proyectos en otros entornos de trabajo (bifurcar) y poseer la certeza de quienes son los inversionistas de los proyectos de la cadena de bloques.

---

[7] Bitcoin: Es una criptomoneda descentralizada que nace el 18 de agosto de 2008. Sirve para intercambiar bienes y servicios en la red *Peer-to-Peer* de manera rápida y segura, implementando la Tecnología *Blockchain*.
[8] GitHub: Plataforma más grande en el mundo. Cuenta con repositorios para desarrollo de software a través de Linux en la comunidad *Blockchain.* Debido a su gran repositorio sobresale de otras plataformas populares como GitLab, SourceForce, entre otras [59].

La tecnología *Blockchain* a pesar de su corto tiempo de existencia, ha llamado la atención de muchas empresas de renombre que apuntan e invierten por la innovación como IBM, Samsung, Amazon, Intel, Chan, el consorcio R3[9]. Esto constituye una nueva alternativa para cambiar el mundo digital, así como Internet en su tiempo cambio la distribución de la información. Con esta concepción *Blockchain* se enfoca en descentralizar la información, sin la necesidad de tener un sitio de control; lo que implica, contar con un sistema seguro y transparente mediante la cadena de bloques.

Blockchain

Blockchain es una tecnología que está formada por una cadena de bloques en la red *peer-to-peer*. Fue lanzada por primera vez su cadena de bloques en 2009[10]. Permite verificar, actualizar y mantener toda la información sincronizada directamente sobre Internet. Elimina la necesidad de contratar alguna institución o entidad para procesar y validar las transacciones. Además, permite almacenar las transacciones cronológicamente, sin la necesidad de modificarlas.

La tecnología *Blockchain* constituye una base de datos distribuida en tiempo real, cuenta con su *ledger* o libro de transacciones virtuales, donde se registran todas las operaciones que hacen los usuarios de la red y van a formar parte del bloque. La programación de esta tecnología se basa en software libre, donde el código se encuentra a disposición de todos los usuarios, para que cualquiera pueda utilizarlo, modificarlo y redistribuirlo de forma gratuita con la finalidad de desarrollar nuevas aplicaciones en diferentes sectores.

La cadena de bloques se basa en un modelo descentralizado de procesos, automatiza la información de forma segura y privada sin necesidad de intermediarios. Está formada por nodos, computadores conectados a la red P2P, que se encargan de verificar las transacciones y almacenar una copia de su registro en la base de datos distribuida global. De esta manera, los miembros de la red conocen los cambios que se han realizado transparentemente, evitando la manipulación o tergiversación de la información [13].

Blockchain maneja *tokens*, monedas secundarias, que representan activos digitales o cualquier valor financiero para pagar directamente por un servicio dentro de la cadena de bloques.

---

[9] Consorcio *R3* (o *R3CEV)*: Es un grupo financiero con más de 80 compañías a nivel mundial, como China Menchants Bank, BBVA, QIWI, BM&F Bovespa, Bank of America Merrill Lynch, entre otros [60].

[10] El 3 de enero de 2009 se minó el Primer bloque en Bitcoin, considerando los principios de la Tecnología *Blockchain*.

Arquitectura

Blockchain maneja una arquitectura *peer-to-peer* sobre Internet. La red está formada por nodos iguales entre sí y brindan servicios en base a consensos entre pares. La información está distribuida en toda la red P2P, todas las transacciones son públicas y encriptadas para evitar manipulación. La decisión de validación es compartida entre todos los miembros de la red lo que garantiza la integridad y robustez frente a ataques. La arquitectura se basa en: una estructura de pilar, en el sistema descentralizado, en el modo de propagación y en el rol de los nodos.

La cadena de bloques se ordena en capas verticalmente, como se indica en la figura 1.4, donde se ve que el primer bloque, bloque génesis, es la base y el resto de bloques están agrupados uno encima de otro, esto indica la altura de la cadena, que está relacionada por el número de bloque. Dentro de la arquitectura por capas se considera a la raíz, al bloque génesis, que sirve de punto de partida desde donde se va a construir todo el resto de la cadena de bloques.

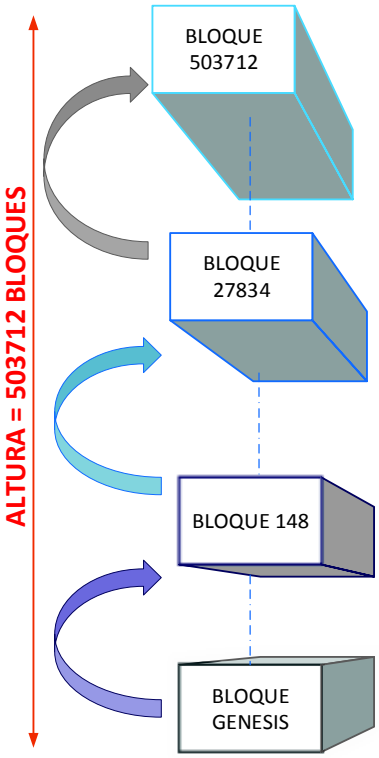

Figura 1.4 Esquema de la cadena de bloques por capas

El sistema descentralizado no necesita de intermediarios, ni de un servicio centralizado. La información está distribuida a todos los nodos en forma autónoma. Si un nodo o múltiples nodos se caen, el resto de nodos mantiene la sincronización de los datos en la red, de esta forma nunca se perdería las transacciones [14].

El sistema descentralizado en la red P2P involucra algunos criterios:

- Cada nodo es el encargado de verificar independientemente cada transacción, teniendo en cuenta su correcta sintaxis y estructura de los datos; el tamaño de la transacción en bytes, número de operaciones y revisar el gas apropiado para la transacción.
- El rol de los nodos mineros es añadir las transacciones a los nuevos bloques por medio del algoritmo de consenso llamado prueba de trabajo.
- Cada nodo es delegado de comprobar los nuevos bloques creados y colocar estos dentro de la cadena de bloques.

Una transacción en *Blockchain* se propaga en *broadcast* a toda la red P2P, donde cada nodo de la red escucha las transacciones y las intercambia con sus nodos vecinos. Este proceso de *broadcast,* permite que todos los nodos de la red sepan la información que está siendo validada y posteriormente sea añadida en el *ledger*.
Los nodos son iguales, pero de acuerdo a la función que cumplen pueden ser nodos simples, encargados de validar, propagar las transacciones y actualizar la copia de la cadena entre sus vecinos sin requerir permisos externos; y nodos especiales, mineros, encargados de crear nuevas transacciones o bloques, en base al algoritmo de prueba de trabajo y su posterior propagación al resto de la red, mantienen también una copia completa de la cadena.

Topología

La figura 1.5 presenta la topología plana de una red P2P, donde varios computadores están interconectados entre sí formando una malla. Cada nodo va descubriendo a otros nodos durante su inicialización y va recogiendo información sobre sus pares distribuidos, a este proceso se le conoce como *flooding* o inundación [15]. Se aprecia que no existe un servidor central ni jerarquía entre los nodos.

Si el nodo A desea enviar su información al nodo D, entonces la información viajará por toda la red entre pares, de modo que el nodo A empieza enviando su información a sus *peers* inmediatos que son el nodo B y nodo C. El nodo B y C propaga su información a todos sus vecinos que se encuentran conectados, ese proceso se sigue sucesivamente hasta que el nodo D reciba la información. Este proceso es abierto y toma unos pocos segundos.

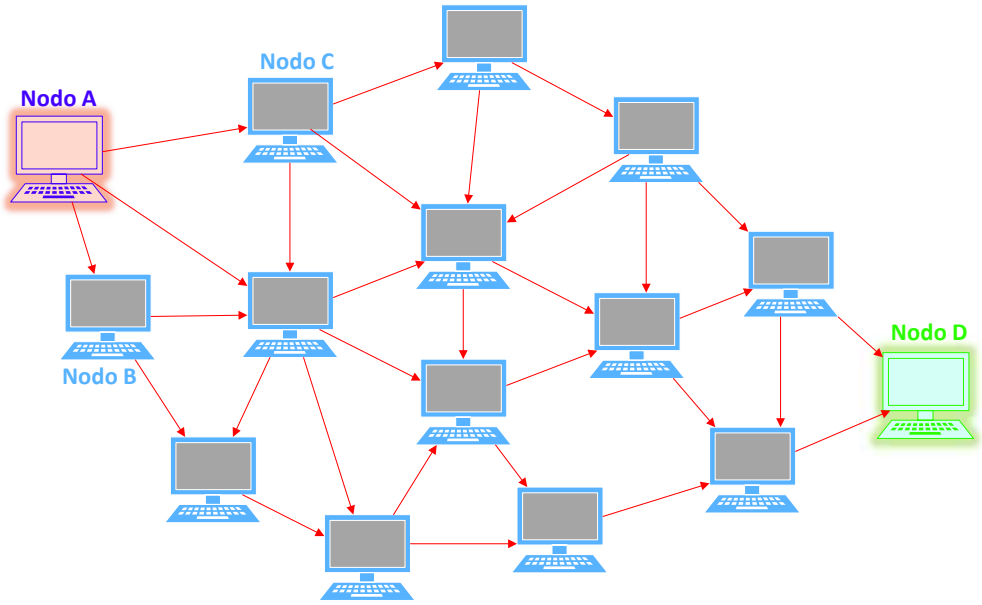

Figura 1.5 Nodos en una Red Peer-to-peer (P2P)

Por ejemplo, si se considera los sistemas bancarios, la responsabilidad de una transferencia seria de toda la red, es decir no existiría una entidad central para procesar y validar la transacción. Cada nodo se encargaría de verificar independientemente las transacciones, una vez validada, propagaría la transferencia a sus vecinos, quienes tendrán una copia de la transacción y la almacenarían en su *ledger*; con un tiempo de espera menor que en el sistema bancario tradicional. Por lo general, en el sistema convencional financiero de transferencia de dinero, el pago de una transacción requiere de una autoridad central "Banco" como intermediario para verificar y procesar el dinero, si la transferencia fuera de otro banco implicaría un mayor tiempo para hacerse efectiva.

Estructura de la cadena de bloques

Blockchain está formada por una cadena de bloques, donde cada bloque contiene un conjunto de transacciones. Las transacciones son almacenadas en el *ledger,* libro de transacciones, y son redistribuidas a todos los nodos que conforman la red, para que se encarguen de validar las mismas.

El bloque está formado por una serie de campos variables, como se indica en la figura 1.6. El tamaño del bloque es de 4 bytes, la cabecera de 80 bytes, el contador de las transacciones es variable (de 1 a 9 bytes) y las transacciones también son variables (alrededor de 250 bytes). Comúnmente un bloque en promedio tiene más de 500 transacciones [15].

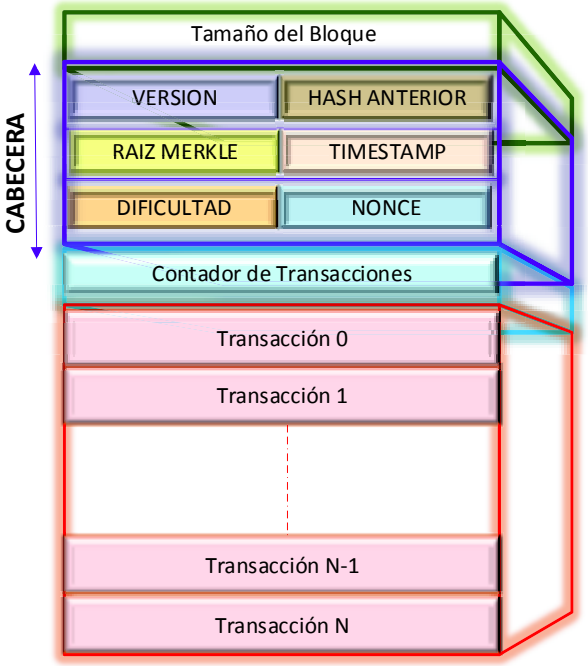

Figura 1.6 Campos de un bloque

Los campos de cabecera del bloque se detallan a continuación [15]:

- Versión o *version*: número de 4 bytes, que indica la versión de software y protocolo. En algunas ocasiones, se usa el término *index*[11].
- Hash[12] anterior o hash padre, *ParentHash*: identificativo de 32 bytes que hace referencia al hash del bloque anterior. De esta forma, se concatena cada bloque de la cadena.
- Raíz de Merkle: indica el hash de raíz del *Merkle Tree*[13] de ese bloque. Trabaja con 32 bytes.
- *Timestamp*: es el sello de tiempo de 4 bytes e indica cuando fue creado el bloque.
- Dificultad o *difficulty*: tiene 4 bytes y muestra el nivel de dificultad para hallar el bloque.
- *Nonce*: contador de 4 bytes que sirve para calcular la función hash.

Por lo general, los tres últimos campos, *Timestamp, difficulty* y *nonce*, sirven para calcular el algoritmo de la prueba de trabajo. Dependiendo de la plataforma donde se implemente la *Blockchain* pueden cambiar la estructura del bloque.

[11] *Index*: Número ascendente que demuestra la posición del bloque en la cadena.
[12] *Hash*: Es la huella digital del bloque, se encuentra en la cabecera e identifica un bloque de forma única e inequívoca. Se origina independiente por cualquier nodo de la red.
[13] *Merkle tree*: Es el árbol binario formado por hashes criptográficos que indica la concatenación de un hash padre con su hijo.

Entramado de bloques

Los bloques se enlazan unos a otros cronológicamente, con referencia al hash del bloque anterior, que está dentro de su propio bloque. El Bloque Génesis tiene un hash previo de 0, ya que no existe un bloque anterior a este. Cada nodo examina la cabecera entrante para revisar el hash previo y mantiene una copia local de la *Blockchain,* que se va actualizando constantemente según vaya creciendo la cadena.

Cuando por primera vez se produce una transacción en la red P2P, se crea un primer bloque en el *ledger* llamado Bloque Génesis, *Genesis Block*. Los siguientes bloques que posteriormente se van a generar, van a ser añadidos al Bloque Génesis para formar una lista de bloques. En *Blockchain*, cada bloque esta enlazado al bloque anterior lo que genera la seguridad y transparencia en la información sobre la red P2P.

La figura 1.7 indica los campos indispensables de una *blockchain* formada por cuatro bloques. El primer bloque que se genera es el Bloque Génesis, cuyo *index* es 0, los siguientes bloques van incrementando su identificar según sea su posición en la cadena. Después está el *Timestamp* que ayuda a mantener el orden cronológico en la cadena; luego sigue el hash que garantiza que nadie pueda crear o insertar un bloque en la cadena, ya que no coincidirían los hashes. El siguiente elemento de la cadena son los datos, que constituye el *input* que se van a almacenar en el bloque, estos pueden ser información, eventos o dinero de una transacción; y finalmente el *nonce*.

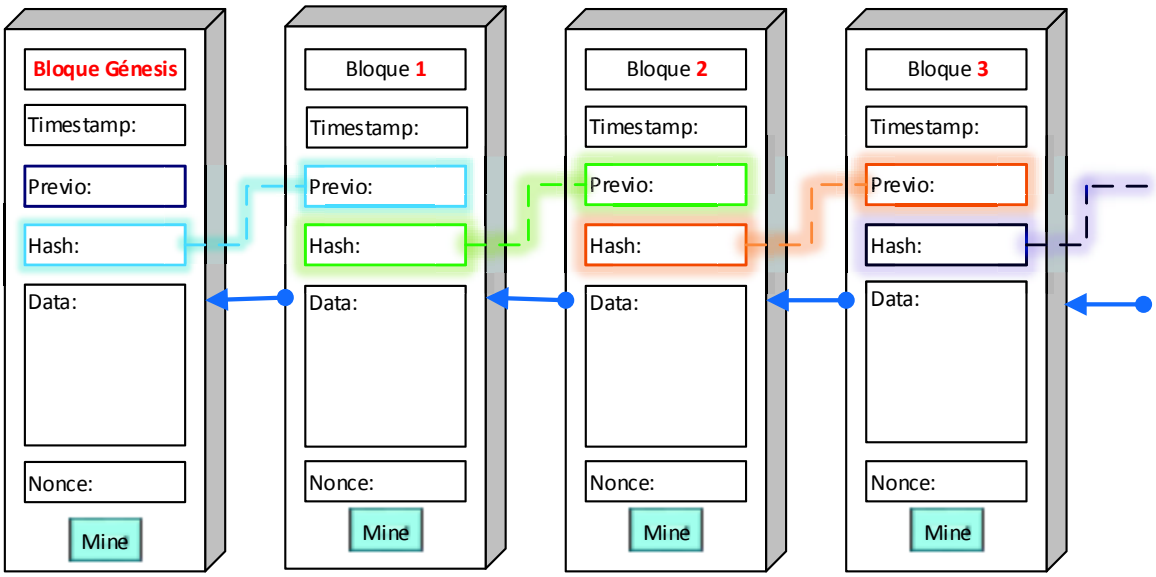

Figura 1.7 Esquema del enlace de la Cadena de Bloques

Considerando la cadena de 4 bloques de la figura 1.7, se interpreta que la altura del bloque es de 3 e indica que éste es el último bloque en la cadena. Además, el bloque 3 dentro de su propia cabecera hace referencia al hash del bloque anterior, que contiene el hash de su padre. Por lo tanto, el *hash* padre afecta a su *hash* hijo en el bloque nuevo.
Si un usuario desea alterar el hash del bloque, cambiando un solo bit o sobrescribir la cadena, dicho cambio solo afectaría al bloque donde se está manipulando la información, por lo tanto, sólo se alteraría ese *hash* actual, esto provocaría una discontinuidad al momento de enlazarse los bloques ya que no coincidirá los *hashes* padre e hijo. Para intentar alterar una cadena sería necesario ir alterando uno a uno cada bloque hasta el origen, algo que requeriría una capacidad de recurso computacional y tiempo.

Algoritmo de consenso

El algoritmo de consenso que aplica la prueba de trabajo para calcular el *hash* en la cabecera es SHA[14]256, trabaja con 256 bits. Este hash es calculado por cada nodo, cuando un bloque ingresa a la red. Toma como parámetro de entrada la cabecera del bloque, es decir trabaja con el *hash* previo del bloque, el *timestamp*, los datos del bloque y el *nonce* para calcular un solo *hash* único [16].

El algoritmo toma los datos de entrada de cualquier longitud y calcula su correspondiente hash de longitud fija y única, se parece a la huella digital de cada persona, es imposible que coincida. El tener éxito en encontrar el *hash* correcto, involucra varias pruebas de trabajo aleatorias que satisfaga la función *hash*.

Para garantizar la confiabilidad de las transacciones, se implementa la prueba de trabajo, *Proof of Work,* que revela que un bloque es válido. SHA256 se implementa durante el proceso de minado, indica que no puede ser alterada la cabecera, sin involucrar una nueva prueba de trabajo, debido a que todos los bloques están enlazados unos a continuación de otro. Por lo tanto, es imposible encontrar dos *inputs* diferentes que produzcan la misma función *hash*.

El primer minero en encontrar la función *hash* retransmite a la red, añadiendo este *hash* en el bloque enviado. De este modo, el nuevo bloque provisionalmente queda enlazado a la cadena de bloques a través de los *hashes*. Si se comprueba que el *hash* es correcto, se almacena en el *ledger*. Mediante *broadcast* se comunica a los otros nodos para que también puedan comprobar y retransmitir a los demás nodos de la red.

[14] SHA (Secure Hash Algoritm): Algoritmo de Hash Seguro, es una función que produce una huella “hash” a partir de una entrada de tamaño arbitrario.

Características de la cadena de bloques

Blockchain es una base de datos pública distribuida en la red P2P, formada por una serie de nodos unidos entre sí por su hash. No necesita de intermediarios para avalar la autenticidad y seguridad de las transacciones. Cada bloque de la red es identificado por su altura y por su hash anterior.

La información que un usuario envía a la red, se ordena en cadena de bloques. Los nodos se encargan de verificar la transacción, por consenso de todos los miembros que participan en la red se valida la información y esta es recibida por todos los nodos de la red. Existe una copia única de la transacción en cada nodo que se actualiza cada vez que se añade un bloque nuevo a la cadena.

Para evitar cualquier manipulación con los datos, las transacciones son públicas y se almacenan en el orden que fueron realizadas, de esta forma la cadena es inmutable, por lo tanto, la cadena de bloques puede ser consultada en cualquier momento por cualquier usuario de la red.

Cuando se descubre al mismo tiempo diferentes bloques por distintos mineros, temporalmente se tiene que un *hash* padre puede tener múltiples *hashes* hijos, a este proceso se llama bifurcación, *fork*, de la cadena. Por medio de la prueba de trabajo se resuelve este problema, ya que un bloque en su cabecera sólo puede tener un hash padre.

La minería permite elegir el siguiente bloque que se unirá a la cadena de bloques, implementando la prueba de trabajo, donde los mineros realizan procesos criptográficos al probar diferentes números aleatorios hasta encontrar la correcta función *hash,* basada en el *hash* anterior contenido en dicho bloque.

La cadena de bloques garantiza la seguridad y confiabilidad en la red, asegura la integridad del bloque por medio de un consenso distribuido de los participantes en la red *peer-to-peer*. Cuando la información se ha validado, no puede ser alterada, ni borrada por ningún usuario en la red [17].

Los mineros por realizar este proceso de consenso reciben una recompensa de Bitcoins, Ether o cualquier criptomoneda[15]. Actualmente, esta compensación es de 12,5 bitcoins[16] o 3 Ethers[17] [18].

[15] La criptomoneda o criptodivisa: Es una moneda digital de intercambio de valor de forma segura, rápida, anónima y descentralizada.
[16] 12,5 Bicoins = 91.400,00 dólares. Tomado de coinmarketcap.com el jueves 9 de noviembre a las 20:12
[17] 3 Ethers = 963,15 dólares. Tomado de coinmarketcap.com el jueves 9 de noviembre a las 20:12

Clave criptográfica

Blockchain maneja una clave criptográfica asimétrica, es decir, trabaja con dos claves una pública y otra privada. La clave que se transmite entre el emisor y el receptor en la red P2P no es conocida, ya que la clave privada se relaciona a la clave pública, esto permite que si la clave es interceptada por algún usuario en la red sea imposible de descencriptar. La clave privada tiene toda la información sobre el usuario de la red, mientras que la clave pública muestra lo que el usuario desea que el resto de nodos vean.

Para una trasmisión, el usuario usa la clave privada, mientras que para recibir solo es necesario la clave pública. De esta forma se conserva el anonimato de los participantes sobre la red, ya que solo se conoce la clave pública del usuario. A pesar de eso, el anonimato no está garantizado totalmente puesto que la cadena de bloques es pública y puede ser rastreable su clave pública a lo largo de toda la red, mientras el usuario siga usando una misma clave durante mucho tiempo se podría saber su identidad real. Para disminuir este seguimiento, muchos usuarios optan por utilizar más de una clave, cambiar con frecuencia o generar las claves por software como *Keypass* o por hardware implementando el *wallet* por medio de Trezor[18] [19].

Clasificación de *Blockchain*

Existen dos tipos de *Blockchain* según sus datos y pueden ser públicas o privadas. Ambas comparten similitudes, como por ejemplo, trabajan bajo un sistema descentralizadas sobre Internet en una red *peer-to-peer*, manejan algoritmos de consenso para sincronizar la información, entre otras [20]. La principal diferencia que radica entre ambas tecnologías se relaciona con el modo de participar en la red, ejecución de protocolos y sincronización en el libro de transacciones, *ledger*.

Blockchain Público

Una *Blockchain* pública es completamente abierta, cualquier persona se puede unir, participar y consultar su información. El usuario que desea participar en esta red sólo sincroniza su nodo a la red principal o *main net* y adquiere los mismos derechos que el resto de participantes. Por ejemplo, libre acceso, no requiere permisos para generar y verificar las transacciones, no existen restricciones para leer la información, puede replicar o minar transacciones dentro de toda la red [21].

[18] Trezor: Dispositivo para generar y guardar claves privadas implementando palabras de semilla, *seed*.

El proceso de minería está abierto para cualquier miembro de la red basado en la prueba de trabajo, *Proof-of-work, PoW*. Un ejemplo de este tipo de red más grande en el mercado digital es Bitcoin, donde el nuevo bloque es añadido aproximadamente cada 10 minutos por un proceso de minado. *Ethereum* es otro tipo de *Blockchain* pública.

Un inconveniente de la cadena de bloques pública es la cantidad de recursos que demanda y el descubrimiento de nuevos nodos; lo que demanda un gran poder computacional para mantener sincronizado el libro de transacciones distribuido, *ledger*. Cada nodo de la red trabaja complejamente para resolver los algoritmos criptográficos y las pruebas de trabajo. Al ser una red pública, no existe mayor privacidad con las transacciones. Por lo tanto, no es recomendable usar estas redes para aplicaciones empresariales.

Blockchain Privado

En la cadena de bloques privada todos los usuarios que conforman la red son conocidos, pero tienen restricciones de acceso, uso de herramientas, participación en la red y gestión de la plataforma. Por lo general, existe una autoridad, equipo, grupo de usuarios o consorcio que restringe el acceso y administra la red. Si un nuevo usuario desea participar en esta red, necesita una invitación o permiso para unirse. Por otro lado, para pertenecer a la red, el usuario acepta las condiciones o el contrato inteligente, *Smart Contract*. El acceso a esta red privada está controlado por los miembros de la red, lo que va a generar un mecanismo de consenso más simple para la verificación de la transacción [22].

Sólo los nodos que conforman la red pueden participar y consultar sus transacciones, es decir, no permite ejecutar transacciones a otros usuarios que no sean miembros de la red. Por lo tanto, la información se intercambia entre los nodos que trabajan en la misma red. El proceso de minado, la verificación de transacciones y bloques, puede ser delegado a un miembro autorizado de la red y cada nodo cumple un rol específico. En este tipo de red privada existe mayor productividad y escalabilidad para realizar aplicaciones en diferentes áreas implementando los contratos inteligentes *Smart Contrats* [23].

Un ejemplo de la *Blockchain* privada es *Hyperledger Fabric* auspiciado *Linux Foundation*, IBM *Blockchain*, Eris/Monax, *Ethereum* privado; *Slack Technologies*, que es una red privada de *Ethereum* Chile.

Plataformas

Las plataformas que trabajan sobre *blockchain* utilizan los mismos principios básicos, código abierto, seguridad, transparencia, eficiencia y validación de todas las partes en la transacción. Según el enfoque del proyecto, añaden nuevas características, codificación de datos en las transacciones e implementan diferentes algoritmos se consenso.

La figura 1.8 indica algunas plataformas competitivas que funcionan con la cadena de bloques en el mercado distribuido, entre las que se destacan: *Bitfury* desarrolla hardware y software para la industria, *Ethereum* se enfoca para desarrollar aplicaciones descentralizadas en base a contratos inteligentes, *Hyperledger* trabaja con los libros contables distribuidas a nivel empresarial, *IOTA* provee infraestructura para *IoT*, Ardor desarrolla contratos inteligentes y Ripple se utiliza para realizar pagos internacionales globales [24].

Figura 1.8 Plataformas que funcionan con la cadena de bloques [25].

Ethereum

Ethereum es una plataforma pública descentralizada que nace en diciembre de 2013 por Vitalik Buterin y otros cofundadores como Gavin Wood y Joseph Lubin; con el propósito de crear aplicaciones en cualquier entorno industrial considerando los principios de la cadena de bloques [26]. El primer bloque minado fue el 30 de Julio de 2014. Por lo tanto, esta plataforma es una herramienta de software libre aplica los principios de la tecnología *Blockchain*, donde corren todas las transacciones. Permite crear cualquier tipo de contratos inteligentes[19] o *smart contracts*; realizar y distribuir aplicaciones descentralizadas (*DApps*).

[19] *Smart contracts*: Programas que almacenan datos y se ejecutan en cada nodo. Actúan como agentes autónomos para compilar la aplicación descentralizada.

Ethereum maneja como *token* el Ether (ETH), que representa un activo digital como forma de pago para un servicio determinado dentro de la plataforma *Ethereum*. Actualmente en el mercado descentralizado, no existe límite de la cantidad de *tokens* que circulan en el mercado digital. *Ethereum* implementa el estándar ERC20 para el costo del *Gas*[20] en la ejecución de un contrato, de esta forma fácilmente los contratos puedan interactuar correctamente con los *tokens* que trabajen con el estándar ERC20 [18].

Ethereum trabaja con el algoritmo de consenso de prueba de trabajo, *Proof of work* y el algoritmo de seguridad que maneja es Ethash. Esta plataforma es más eficiente ya que su latencia es menor, para la creación de bloques se demora aproximadamente 16 segundos en comparación con Bitcoin que se tarda 10 minutos.

Por lo general, se usa esta red *Ethereum* para trabajar con gran flujo de información en el *ledger* a través de bucles. Las aplicaciones que se crean tienen un medio confiable, ejecutando contratos inteligentes automáticamente, sin necesidad de depender de terceros. Los contratos se ejecutan en esta plataforma en su máquina virtual, Ethereum Virtual Machine (EVM) e implementa un lenguaje de programación por *Turing Complete*.

Las transacciones llevan la información, se miden en bytes. El tamaño del bloque no está definido en *Ethereum* pero en promedio es menor a 1Mb[21]. Además, las transacciones se realizan en bloques, se encadenan usando un *hash* y son verificadas por los mineros, quienes reciben incentivos de 3 *Ethers* por validar el bloque. A diferencia de la tecnología *Blockchain* en *Ethereum* el minero o grupo de mineros (*pool*s), puede validar las transacciones o contratos inteligentes, quien realice este proceso en el menor tiempo recibe una recompensa en Ethers [4].

Las transacciones tienen un costo en Ether que varía dependiendo del *Gas Price*[22] para ejecutar la aplicación. El minero verifica el *Gas Price* y da prioridad a esa transacción del resto de transacciones que se generan en la red P2P. Un costo elevado de gas en una transacción garantiza mayores posibilidades de seleccionar esa transacción por los mineros. Cada transacción tiene un límite de *Gas* a pagar llamado *Gas Limit*.

El proceso de minar implica un menor consumo energético ya que se basa en el ancho de banda y no en el *hashrate*[23], también implica un menor tiempo de respuesta[24] para validar

---

[20] *Gas*: Es el coste computacional para procesar un determinado número de transacciones.
[21] En Bitcoin en tamaño del bloque es de 1Mb (1048576 bytes), lo que hace que las transacciones, los bloques y la cadena de bloques sea más pesada.
[22] *Gas Price* o precio del gas: Es una tarifa en Ether que se paga para ejecutar, validar y añadir la transacción o el contrato inteligente a la cadena de bloques, todo este proceso involucra un gasto computacional.
[23] *Hashrate*: Es el valor que se obtiene del número de cálculos del hash en un periodo terminado [Mh/s].
[24] Tiempo de respuesta: Relación entre la frecuencia de emisión de la criptomoneda y la velocidad de la red.

y añadir el bloque a la cadena en 16 segundos, es decir son procesadas casi instantáneamente.

Las unidades de *Ethereum* están subdivididas en pequeñas cantidades de decimales como se muestra en la tabla 1.1 en orden descendente. La unidad típica usada para las transacciones es *Wei* que representa 18 decimales de *Ether*. Todas estas denominaciones provienen de nombres científicos usando el Sistema Internacional de Unidades (SI) o nombres comunes.

Tabla 1.1 Nombre de las Unidades de *Ethereum* [27]

Decimales	Nombre Coloquial	Nombre SI
1^{6}	---	Megaether
1^{3}	Grand	kiloether
1	Ether	Ether
1^{-3}	Finney	Miliether o mili
1^{-6}	Szabo	Microether o micro
1^{-9}	Shannon	Gigawei o nanoether
1^{-12}	Babbage	Megawei o Picoether
1^{-15}	Lovelace	Kilowei o femtoether
1^{-18}	Wei	Wei

ERC20

ERC, *Etherium Request for Comments,* es un protocolo para los *tokens* que garantiza la interoperabilidad entre ellos; define un conjunto de métodos y reglas para su funcionamiento. ERC20 es el estándar más conocido en todas las plataformas, con una acogida del 99% en el mercado digital y por su interoperabilidad con otros *tokens* que tengan como base el estándar, sin importar, el tipo de aplicación o la plataforma de desarrollo [28].

ERC20 permite crear contratos inteligentes, que se ejecuta sobre la plataforma de *Ethereum*, con una alta confiabilidad, ahorro de recursos y tiempo. El estándar ERC20, no es una moneda digital, más bien es un valor virtual. Representa un activo digital específico que se transmite dentro de la cadena de bloques. Se puede integrar a los proyectos, ICOs[25] o aplicaciones descentralizadas.

ERC20 facilita la funcionalidad entre *Dapps* y *wallets* aunque manejan diferentes *tokens* a través de múltiples plataformas. Esta interfaz permite que los *tokens* implementan los mismos parámetros básicos, como son, métodos y eventos [29].

[25] ICO: Es una oferta inicial de moneda que financia y comercializa un proyecto de forma pública a través de *tokens* en aplicaciones descentralizadas.

Monedero

El monedero o *wallet* guarda la clave privada del usuario y trabaja directamente con los *tokens* compatibles con el estándar ERC20. Se usa para enviar, recibir y guardar *Ethers*. Trabaja con diferentes tipos de carteras, dependiendo de su complejidad y características como: móviles *(mobile wallet*), de escritorio (*desktop wallet*) o basado en la web (*web-based wallet*). Dentro del *mobile wallet* se puede trabajar con *MetaMask,* se usa para realizar pruebas debido a su facilidad de manejo, es capaz de conectarse a una gran variedad de nodos de *Ethereum* y a su cadena de bloques.

Jaxx, Mist, Parity son carteleras de escritorio multiplataforma para una variedad de sistemas operativos como Windows, Mac, Linux, iOS y Android. Esta opción es perfecta para usuarios nuevos debido a su simplicidad y facilidad de uso. Finalmente, la cartelera basada en la Web son *MyEtherWallet* (MEW) y *MetaMask* que se pueden ejecutar en cualquier navegador. *MetaMask* permite trabajar con Firefox o con una extensión de Chrome. También existen los monederos físicos, como son el *Trezor* y *Legder*, que requieren la adquisición de un hardware adicional y pueden también interactuar con los monederos de la web.

Algoritmo de seguridad

Ethereum implementa a parte del algoritmo de consenso, el algoritmo de seguridad llamado Ethash, consiste en una mezcla de protocolos SHA3, que facilitan el proceso de minado. *Ethereum* usa el protocolo de consenso *GHOST*[26] para asegurar la cadena y minimizar la posibilidad de ataques, debido a que el tiempo de generación de los bloques inicialmente era de 60 segundos, pero implementando el protocolo se redujo su valor a 16 segundos, lo que provoca mayores riesgos de bloques huérfanos o incorrectos; esto produce que se limiten la cadena y se recalculo de la dificultad cada 1 bloque [30].

Debido a la complejidad del protocolo, a la dificultad de la aplicación y al creciente número de participantes en la red se necesita aumentar los requerimientos de hardware. Para manejar gran volumen de información como en los sistemas financieros, para el proceso de minado se requiere contar con un hardware especial que es un procesador GPU[27] (Unidad de Procesamiento Gráfico).

---

[26] Ghost (*Greedy Heaviest-Observed Sub-Tree*): Se base en el árbol de bloques, que mantiene un umbral del 50% en el hash, si se producen ataques y retardos extremos, manteniendo un alto rendimiento en las transacciones.

[27] Procesador GPU (Graphics Processing Unit): Es una tarjeta gráfica que aliviana la carga de trabajo del procesador en aplicaciones como videojuegos o aplicaciones 3D interactivas.

Prueba de Trabajo o *Proof of Work*, PoW

Ethereum lanzó en el 2009 este algoritmo de consenso en el mercado e implementó los principios de *Blockchain*, mediante la prueba de trabajo. Básicamente, los mineros compiten para encontrar la función correcta hash y añadir ese bloque en la cadena a través de la resolución de complejos problemas matemáticos.

El enfoque de la *PoW* es garantizar la seguridad y confiabilidad a través de los mineros que validan los bloques, sin embargo, implica problemas de latencia, mayor gasto eléctrico y computacional. Además, trae consigo un impacto negativo en el minero, ya que demanda mayores recursos de hardware. Por lo general, para realizar el proceso de minado sólo es necesario trabajar con un CPU o GPU, ningún equipo más se puede utilizar en esta tarea. Las plataformas más populares que trabajan con la prueba de trabajo son Bitcoin, Ethereum, Litecoin, entre otras [31].

Prueba de Participación o *Proof of Stake,* PoS

La prueba de participación aún está en estudio para futuras aplicaciones en la plataforma de *Ethereum*. Su objetivo primordial es mejorar el alto coste eléctrico y de hardware que conlleva la prueba de trabajo, PoW. Considerando este nuevo enfoque, los mineros no son los encargados de aceptar los bloques, si no los validadores[28], quienes van a realizar el proceso de validación de bloques poniendo en juego sus propios *Ethers*. Si la transacción es válida, se reparte equitativamente la comisión entre todos los validadores.

En cambio, si los validadores aprueban un bloque inválido o actúan maliciosamente perderán sus tokens. Este proceso da mayor responsabilidad a los validadores quienes invierten sus propias criptomonedas. También implica un mayor riesgo para quien quiera atacar la red. Los *tokens* que ya trabajan con PoS son: Peercoin (PPC), Stratis (STRAT), Neo (NEO), Bitconnect (BCC), entre otras [32].

Contrato Inteligente

El contrato inteligente es un acuerdo autónomo entre las partes que conforman la red. El *Smart Contract* contiene una serie de programas informáticos que se ejecutan automáticamente. La autoejecución del contrato está a cargo de la red que usa algoritmos de consenso para reproducir el script del contrato instantáneamente sin intermediarios.

[28] Validadores: Usuarios que tienen tokens y están dispuestas a usar parte de estos (Ethers) para sumar el bloque a la cadena de bloques validados a través de algoritmos matemáticos.

El sistema descentraliza permite que los *Smart Contracts* automaticen sus servicios en cualquier sector industrial de forma segura, transparente y eficiente, sin tener la necesidad de usar un registro centralizado, como se muestra en la figura 1.9, donde los miembros de la red aceptan los términos del contrato sin tener que conocerse, pero de forma pública, manteniendo la privacidad de los usuarios en toda la red.

Figura 1.9 Esquema de un contrato inteligente [33]

Los contratos inteligentes en *Ethereum* se programan en *Solidity*, lenguaje de programación similar a JavaScript y C, facilita su compilación y ejecución en la red P2P. La sintaxis de este código se puede trabajar localmente con la máquina virtual y luego se sube a la red descentralizada *Ethereum* para realizar las pruebas correspondientes en un ambiente descentralizado.

Lenguaje de programación

El lenguaje de programación impide que la cadena de bloques sea hackeada. *Ethereum* utiliza el lenguaje de programación "*Turing complete*", que codifica y calcula la cadena de bloques por comandos e instrucciones. Maneja siete lenguajes de programación entre los que se destacan Solidity[29], Serpent[30], JavaScript, HTML y Python, lo que aumenta su complejidad.

Sin embargo, independiente del lenguaje de programación a considerar para el desarrollo del contrato inteligente, la plataforma Ethereum trabaja con un lenguaje de máquina, es decir, la compilación no está a cargo del desarrollador, sino que el compilador se encarga de ejecutar el contrato y asignar espacio en la memoria.

[29] Solidity: Es el lenguaje oficial de la plataforma Ethereum. Maneja una compleja de programación basada en una estructura de datos que emplean funciones y métodos; similar a Javascript [61].
[30] Serpent: Lenguaje de programación de alto nivel parecido a Python. En las primeras etapas fue considerado como el lenguaje script principal.

Redes de prueba o *Testnets*

Ethereum usa redes de prueba para experimentar nuevas aplicaciones descentralizadas o realizar actualizaciones, sin tener que invertir *Ethers*. Como es una *testnet* no requiere gastar el *gas*, ya que no tiene ningún valor comercial.

La figura 1.10 indica las redes de prueba que se pueden correr en *MetaMask*[31], como son en las redes de *Ropsten* o *Ropsten Test Network, Rinkeby*. Esta plataforma interactiva permite crear y administrar las transacciones en la cadena de bloques de manera segura, además trabajan con el algoritmo de consenso por prueba de trabajo.

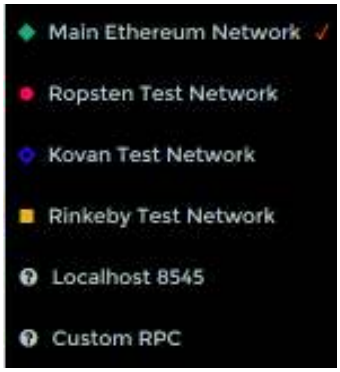

Figura 1.10 Redes de prueba para *Ethereum*[32]

Si se desea usar en la red principal, *Main Ethereum Network*, los *Ethers* que se inviertan en las pruebas si van a ser descontados de la cuenta del usuario, debido a que es similar como si se estuviera trabajando en la red real de *Ethereum*.

La figura 1.11 indica la red *Kovan* en *Metamask*, esta es la única red de prueba que permite trabajar con el algoritmo de prueba de autoridad, *Proof of Authority*, e implementa la firma federada. Los Ethers en esta red pública no se van a descontar de la cuenta.

Figura 1.11 Red de prueba con Kovan en MetaMask

[31] *Metamask*: Es una herramienta, que proporciona una interfaz al usuario para aprobar o rechazar *Dapps* o transacciones tan sólo con instalar su extensión en el navegador de Chrome, desde https://chrome.google.com/webstore/detail/metamask/nkbihfbeogaeaoehlefnkodbefgpgknn

[32] La figura 1.10 y 1.11 fueron tomadas de https://metamask.io/

Ventajas y desventajas

Ventajas

- *Blockchain* mantiene un consenso distribuido de la información, esto permite que cualquier usuario de la red pueda verificar en cualquier instante sus transacciones. Cada nodo posee una copia de la cadena de bloques.
- La generación de los bloques se realiza de forma descentralizada, pero bajo el consenso de todos los miembros de la red P2P para validar la información. Esto elimina posibles fallas y evita la necesidad de contratar a terceros.
- La seguridad de la red es garantizada por los algoritmos criptográficos, inviolables, mediante sus claves criptográficas que permiten crear, modificar, compartir y almacenar la información.
- Los procesos de autenticación en la red son muy robustos, ya que el usuario maneja su llave pública para ser identificado en la red; mientras que su clave privada sólo es administrada por el usuario. Este proceso mantiene el anonimato y privacidad de todos los nodos de la red.
- *Blockchain* al trabajar con una red P2P, lo que garantiza redundancia de sus datos, que es inherente a través de la replicación de la información y la copia de las transacciones entre los nodos vecinos que conforman la red.
- Los principios de *Blockchain* respecto del funcionamiento, eficiencia, escalabilidad e integridad del servicio, se pueden implementar en cualquier plataforma descentralizada y que trabaje con código abierto.
- Es una red de fácil y útil, que no requiere que los miembros que conforman la red tengan un conocimiento previo de esta tecnología. Para crear una cadena de bloques sencilla, no se requiere gran potencial computacional para su implementación y funcionamiento.
- Crea una oportunidad de innovación y cambio en los servicios para los diferentes sectores industriales dentro del mercado digital. Con la distribución de la información sobre Internet, se pueden establecer proyectos o aplicaciones descentralizadas de forma automática, sin intermediarios y sin posibilidades de estafa.

- La gran mayoría de aplicaciones descentralizadas de *Blockchain*, se centran al ámbito financiero. Por otro lado, no impide que se desarrollen otros proyectos enfocados a otro valor digital que se transfiera en la red *peer-to-peer*. Los principios básicos de esta tecnología siempre garantizan a todos los miembros de la red la confiabilidad de su información, seguridad y anonimato.

- La cadena de bloques maneja un sistema descentralizado, transparente y seguro, que mejora los servicios y productos de los sistemas centralizados tradicionales. Los sistemas de hoy en día, almacenan la información en servidores centralizados que pueden sufrir ataques o demandan un alto costo.

Desventajas

- No existe un control gubernamental para la identidad de los usuarios o de las transacciones, por tanto pueden ser utilizadas para fines de negocios turbios, como narcotráfico o terrorismo.

- Al ser una tecnología joven, aún le falta madurez en el mercado. Esto limita su potencialidad para el desarrollo de aplicaciones descentralizadas en otros sectores diferentes al financiero.

- Para que la tecnología *Blockchain* se imponga en el mercado, falta romper algunos paradigmas y realizar más proyectos enfocados al sector de telecomunicaciones, para que pueda competir con los sistemas convencionales de comunicaciones.

Aplicaciones descentralizadas

Hoy en día, las *apps* son muy familiares para toda la gente, ya que cualquier usuario puede descargar y ejecutar estas en su dispositivo móvil. Actualmente, estas apps en el mercado son centralizadas, donde la información permanece en un servidor o banco y puede ser propenso a sufrir ataques o dejar sin servicio a los usuarios durante horas.

La figura 1.12, tomada del portal *Downdetector*, indica el problema técnico que sufrió Twitter el 17 de abril; el pico más alto fue a las 9H50, con 6.385 reportes de fallas en el servicio a nivel mundial. Resolver el problema tomó alrededor de 2 horas. El Anexo I, indica otros casos de fallas técnicos en los sistemas centralizados.

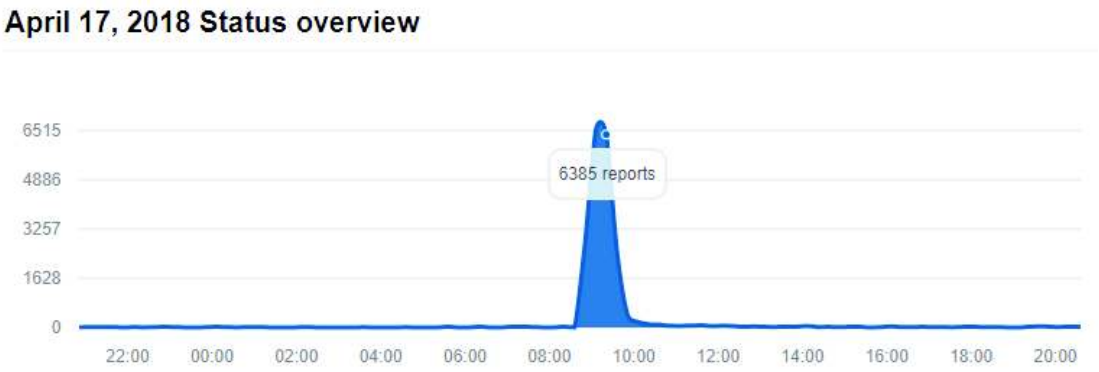

Figura 1.12 Falla técnica del sistema centralizado en *Twitter* [34]

Este tipo de caídas de servicio no se presentarían en *Ethereum,* ya que trabaja con aplicaciones descentralizadas, *Dapps,* donde el contenido de la base de datos está distribuido en toda la cadena de bloques, sin la necesidad de contar con servicios centralizados como servidores o entidades financieras.

La figura 1.13 muestra los sectores donde se están desarrollando aplicaciones descentralizadas; existe un gran impacto en el campo financiero y gubernamental, así como en la salud, seguros y entretenimiento. Falta aún invertir en las áreas, como energía y tecnología. Por lo tanto, la cadena de bloques ha tenido un impacto progresivo en el mercado digital, donde poco a poco se está transformando los modelos centralizados de negocios, en diferentes ámbitos sociales, económicos y tecnológicos.

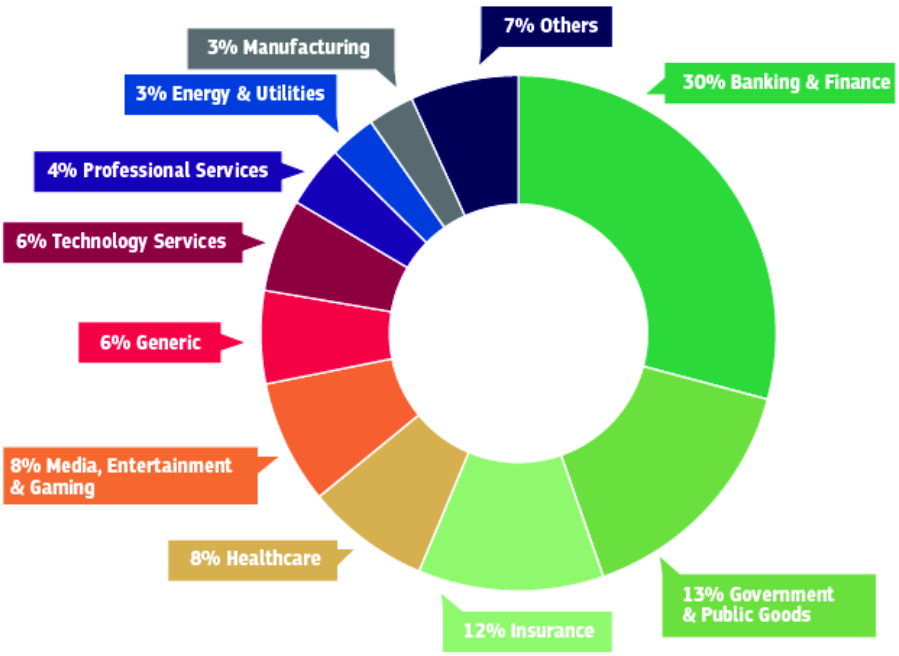

Figura 1.13 Diagrama de las aplicaciones descentralizas en sectores industriales [35].

Aplicaciones en el sector de Telecomunicaciones

Actualmente, en el mercado descentralizado existen infinitas aplicaciones de la cadena de bloques en el sector financiero. La mayoría de Dapps han sido impulsadas por contribuciones, patrocinios y alianzas estratégicas con grandes empresas. De la misma manera, se abren mayores oportunidades para otros sectores industriales, donde las exceptivas y confianza por la tecnología *Blockchain* continúan creciendo cada día.

A continuación, se van a mencionar algunos proyectos con respecto al sector de Telecomunicaciones, que han permitido gestionar los procesos de manera transparente, segura y eficaz:

- **Sistema de almacenamiento en la nube:** en el mercando convencional, existen algunos servicios de almacenamiento en la nube como es el caso de *Dropbox* o *Google Drive*, pero son centralizados. La tecnología *Blockchain* brinda ese servicio, pero bajo un ambiente distribuido, por ejemplo, Storj permite que los usuarios alquilen el espacio que no utilizan a otros y almacenen sus archivos en la nube. Airbnb y Filecoin, alojan y alquilan espacio sobre Internet sin depender de un servidor central, con una fuerte encriptación extremo a extremo. *Litecoin*, trabaja sobre la red P2P para almacenar los datos de manera eficiente [36].

- **Sistema para programación:** existen varios proyectos inspirados en la cadena de bloques, para que los desarrolladores creen o corran aplicaciones descentralizadas, así como, *Lisk* programación en JavaScript para *Dapps*. *Blockcypher*, permite desarrollar proyectos la interfaz de programación de aplicaciones (API). *Devcoin*, está enfocada a apoyar a todo tipo de los programadores de código abierto. *Truffle*, permite que los desarrolladores realicen pruebas de activos sobre Ethereum.

- **Sistema de prestación de servicios:** existe gran oportunidad en el mercado para la prestación de servicios implementando soluciones descentralizadas. *TransActive Grid,* permite trabajar con la energía renovable dentro de un ecosistema seguro, versátil y barato. *e-Chat*, *Messenger* multitarea descentralizado. *FollowMyVote*, herramienta que desarrolla *Dapps* para mejorar la integridad de los votos en tiempo real, donde todos los usuarios conocen los resultados transparentemente, de esta forma se solucionarían muchos casos de manipulación de la información. *Wickr Inc*, medio de mensajería sobre la cadena de bloques donde la información es encriptada en el receptor para evitar la manipulación de la información.

Digital Asset, mejora el procesamiento, eficiencia y distribución de los datos encriptados. [37].

- **Sistema de inteligencia artificial:** *Securecoin,* es una *ICO*[33] cuyo enfoque se da para el ámbito de la seguridad de redes. *IOTA* trabaja con los desafíos que conlleva el Internet de las cosas, *IoT*, donde los dispositivos electrónicos se podrán conectar a través de Internet y realizar acciones automáticamente. En cambio, la plataforma de *Cambridge Blockchain LLC*, permite identificar a los usuarios biométricamente manteniendo una base de datos distribuida y al mismo tiempo respetando la privacidad de los datos del usuario. *Sensormatic Electronic*, maneja las credenciales de los usuarios dentro de los monederos digitales, para facilitar el acceso a las empresas [38].

- **Sistema de comunicaciones entre dispositivos**: el proyecto de *Phuket*, gestiona aplicaciones para *smartphones*. *ShoCard,* protege y optimiza la comunicación entre dispositivos móviles por medio del sistema distribuido de *Blockchain*. *EtherAPIs* se encarga de realizar llamadas remotas a través de un software determinado. *Forcepoint LLC*, aplicación distribuidad que registra el uso del usuario con respecto a los teléfonos inteligentes, computadores personales y cualquier dispositivo conectado a la nube. *nChain*, permite la comunicación implementando claves criptográficas para interconectar dispositivos por medio de procesos de cifrado y firmas digitales. *Cisco Technology Inc*, facilita la gestión de usuarios y la transferencia de contenido entre dispositivos archivados en un registro público e inmutable ordenado cronológicamente. *Bitfury*, brinda soluciones para todo tipo de empresas u organizaciones, promoviendo activos digitales mediante la cadena de bloques ya sea hardware (circuitos o elementos electrónicos, servidores o construcción de *data center*) o software (servicio de domótica, redes o propiedad intelectual). Finalmente, la plataforma *Bank of America Corporation*, colabora con niveles de seguridad y autorización de acceso para el procesamiento de datos de los dispositivos [39].

[33] ICO (*Initial Coin Offering*): Herramienta que permite crear proyectos sobre la cadena de bloques con la ayuda de inversionista de compañías, empresas u organizaciones que brindan un servicio; está basados en *tokens* que por lo general trabajan con el estándar ERC20.

Terminología de *Blockchain* [15] [40]

- **Algoritmo de consenso.** Conjunto de métodos lógicos que se implementan en la red P2P por sus participantes para ejecutar el proceso de minado.
- **Altura del bloque.** Número que indica la cantidad de bloques que forman la cadena de bloques.
- **Bloque Génesis.** *Genesis block*, primer bloque de la cadena de bloques, que se usa para inicializar una red en particular.
- **Bloques.** *Blocks*, conjuntos de transacciones que se enlazan a través de códigos alfanuméricos para formar la cadena de bloques. Un bloque tiene un conjunto de información como la cabecera y las transacciones.
- **Cadena de bloques.** *Blockchain*, lista de bloques que se ordenan a través de los *hashes*, interconectados a su predecesor hasta llegar al bloque génesis y contienen información.
- **Cabecera del bloque.** Forma parte de la estructura del bloque donde se incluye su información como: hash padre, árbol de *Merkle*, *timestamp,* dificultad y *nonce*.
- **Cartera.** *Wallet* o monedero. Software que permite administrar y almacenar activos digitales.
- **Consenso.** *Consensus*, proceso que se produce cuando varios nodos tienen el mismo bloque localmente que se añade a la cadena de bloques.
- **Contrato inteligente.** Script sencillo que se ejecuta automáticamente y todos los miembros de la red son los encargados de validar el resultado, sin necesidad de intermediarios.
- **Cuenta.** *Account,* es parte del estado de *Ethereum*, que tiene un saldo intrínseco. Tiene una dirección única que la identifica del resto.
- **Datos.** *Data,* son los bytes donde se envían los datos del mensaje. Su tamaño es ilimitado.
- **Dificultad.** *Difficulty,* valor que corresponde al nivel de dificultad para la transacción del bloque. Se calcula en función de la dificultad del bloque anterior y del *timestamp*.
- **Dirección.** Lugar donde se reciben las transacciones en la cadena de bloques**.** Está formada por 160 bits.

- **Ethash.** Algoritmo de la prueba de trabajo para *Ethereum* 1.0.
- **Ether.** ETH, criptomoneda de *Ethereum,* que se usa para pagar el *Gas* cuando se ejecuta el Contrato Inteligente.
- **Evento.** Permite usar las funciones de registro de EVM.
- **EVM.** *Ethereum Virtual Machine*, máquina virtual que ejecuta una serie de instrucciones en bytecode. Mecanismo contable para medir el consumo del Gas y limitar el consumo energético.
- **Fork.** Bifurcación es una cadena de bloques alternativa a la original que se produce por caso de error en el sistema.
- **Gas Limit**. Monto máximo del *Gas* para ejecutar la transacción.
- **Gas Price.** Valor a ser pagado en unidades de *Wei* por el costo computacional incurrido como resultado de la ejecución de la transacción o contrato inteligente.
- **Gas**. Moneda virtual usada en *Ethereum* para calcular la ejecución del contrato inteligente.
- **Hash.** Huella digital de longitud finita de los datos producida por la función hash.
- **Hash previo.** Valor que se encuentra en la cabecera del bloque, que enlaza secuencialmente toda la cadena.
- **Libro de registro.** *Ledger*, libro digital donde se almacenan cronológicamente todas las transacciones de la cadena de bloques.
- **Minería.** Proceso para validar los bloques de las transacciones, encuentra el hash válido y lo agrega a la cadena de bloques.
- **Mineros.** *Miners*, nodos especiales de la red u ordenadores potentes y con gran capacidad de computación. Verifican las transacciones en la red P2P, implementando la prueba de trabajo para validar las nuevas transacciones resolviendo problemas matemáticos. Cuando la información se ha validado, no puede ser alterada, ni borrada por ningún usuario en la red.
- **Nodo.** *Node*, ordenador o cualquier dispositivo conectado a la red, que almacena y distribuye una copia actualizada en tiempo real de la cadena de bloques. Un nodo que tiene la función de validar nuevas transacciones.

- ***Nonce***. Número arbitrario que es utilizado una única vez, es igual al número de transacciones enviadas por el emisor.
- **Prueba de participación.** *Proof of Stake* o *PoS*, método por el cual los validadores aceptan las transacciones por un consenso distribuido invirtiendo una cantidad de sus monedas.
- **Prueba de trabajo.** *Proof of Work* o *POW*, verifica que el *nonce* encaje con la función *hash* del bloque. La prueba de trabajo se realiza a través de los mineros que necesitan de gran poder computacional.
- **Raíz de Merkle.** Valor que hace referencia al *hash* de donde proviene.
- **Recompensa.** Cantidad o valor que se extiende al minero como incentivo al encontrar la solución a la Prueba de Trabajo.
- **Red.** *Network*, conjunto de nodos que participan en la red peer-to-peer que sirven para propagar las transacciones y bloques dentro de esta.
- **Retransmisión.** Mediante *broadcast* se transmite a los nodos cercanos la transacción y la verifican; si es correcta la almacenan momentáneamente en una lista de transacciones y se retransmite a cada uno de nodos de la red. Caso contrario, si la transacción no es correcta, se descarta y no se almacena en el registro, esperan al siguiente bloque para volver a realizar las comprobaciones respectivas.
- ***Timestamp*.** Este valor es la marca de tiempo que identifica el instante en que fue creado el bloque.
- **Transacción.** *Transaction*, se produce cuando cualquier usuario que es representado por un nodo transmite la información o valor entre los nodos de la red. Las transacciones son procesadas por los mineros para posteriormente ser incluidas en el bloque de la cadena.
- **Whitepaper.** Documento que describe en detalle los fundamentos básicos de la tecnología *Blockchain.*

2. METODOLOGÍA

El presente proyecto se centra en un estudio técnico del análisis de la utilización de la Tecnología *Blockchain* “Cadena de Bloques” para la gestión de la información de los eventos generados en los sistemas de alarmas residenciales. Este modelo descentralizado fortalece la convivencia y organización vecinal. De la misma forma, permite mejorar el nivel de seguridad de los dueños de las casas contando con un sistema confiable, seguro, de fácil uso y eficiencia.

Se realiza una investigación explicativa, adaptativa y explorativa. Explicativa, para abordar los conceptos fundamentales de la cadena de bloques sobre la plataforma *Ethereum*. Una investigación adaptativa para aplicar los principios de la tecnología *Blockchain* en el sistemas de alarmas residenciales convencionales [41]. Finalmente, se recurre también a la investigación exploratoria, ya que analizara el estándar ERC20 dentro de los sistemas de alarma descentralizados que han sido poco desarrollados en el ámbito de las Telecomunicaciones [42].

Las técnicas e instrumentos para recolectar información que se emplean en este estudio son la consulta, la observación y la experimentación. Se recurre a las consultas de fuentes y revistas científicas, así como, de artículos para recopilar la información sobre la tecnología *Blockchain* y la plataforma *Ethereum*. El análisis de documentos ya sea por materiales impresos o Internet permite recopilar la información de los sistemas descentralizados. Por otro lado, la observación ayuda a identificar los puntos estratégicos, zonas y sensores a utilizarse en el sistema de alarmas residenciales. En cambio, la experimentación facilita la simulación de los nodos sobre la red P2P a través de la plataforma descentralizada privada *Ethereum* para la gestión de eventos del sistema de alarmas residenciales [43].

Este proyecto tiene las siguientes fases metodológicas de diagnóstico, análisis de gestión de la información y costos. La fase de diagnóstico, indica los requerimientos de los sistemas de alarmas residenciales de 30 casas en un medio centralizado, así como, en un ambiente distribuido basado en la tecnología *Blockchain.* En la siguiente fase de análisis se compara la gestión de los eventos del sistema tradicional y como se realizará este servicio en el nuevo sistema de alarmas descentralizado de 30 usuarios residenciales en un esquema P2P con la red privada *Blockchain*. Finalmente, en la fase del análisis de costos se presenta los gastos que conlleva implementar el sistema de alarmas convencional y el nuevo sistema de seguridad con la utilización de la tecnología *Blockchain*.

2.1. Fase de diagnóstico

Requerimientos para el sistema de alarmas residenciales tradicional

Los requerimientos para el sistema tradicional de alarmas que se mencionan a continuación, se tomaron como referencia de la Secretaria de Seguridad y Gobernabilidad del DMQ [44], y la política de seguridad del Ministerio del Interior [45]:

- Se requiere el servicio de monitoreo de alarmas para 30 casas. Para este estudio, se parte de una construcción moderna de tres niveles. Actualmente, este tipo de casas tienen mucha demanda en el mercado de la construcción [46], donde cada metro cuadrado de la vivienda esta estratégicamente distribuido. La residencia consta de 3 dormitorios, dos baños, sala, sala de estar, comedor, cocina y terraza. Posteriormente, se van a detallar los ambientes para evaluar la cantidad de sensores por espacio.
- Es necesario que cada casa cuente con instalaciones y equipo de alarmas contra intrusión. Adicionalmente se requiere que la empresa proveedora del servicio de monitoreo realice una supervisión continua mediante llamadas. En caso de emergencia el auxilio será de forma inmediata, dependiendo de la distancia entre la empresa y las casas. Por lo tanto, el tiempo de respuesta es variable, pero se estima un máximo de 15 minutos.
- Se requiere asistencia las 24 horas y los 365 días del año.
- La empresa proveedora del servicio debe cubrir el perímetro de la casa; es decir, verificar el estado de puertas y ventanas. De tal manera, que el sistema alerte al usuario, si hay algún foco de ingreso que no se encuentre cerrado al momento del armado, ya sea para abandonar el hogar o para el armado en modo presencial (nocturno).
- Se requiere un detector de humo en la cocina y botones de pánico dispuestos en sitios estratégicos de la casa. Además, se requiere una sirena exterior.
- El requerimiento del sistema de alarmas, es contar, con un servicio centralizado; donde los usuarios de cada una de las 30 casas, realizan la contratación de una empresa especializada en seguridad, para el monitoreo y mantenimiento mensual.
- La operación técnica del sistema de alarmas se verifica periódicamente por la empresa privada y cuenta con el apoyo conjunto del personal de la UPC zonal.
- El análisis de costos toma en cuenta los equipos, materiales, mano de obra y accesorios para el sistema de alarmas de la casa tipo.

Situación actual de los sistemas de alarmas en los hogares

Actualmente, debido al alto índice de inseguridad que se registra en los últimos años, según el Observatorio Metropolitano de Seguridad Ciudadana (OMSC), la capital ha registrado un mayor número de robos y hurtos a la propiedad. Una gran parte de estos eventos, se registra cuando las personas no están presentes en sus hogares [47].

La figura 2.1 detalla los datos de denuncias de robos con asalto (uso de violencia o amenazas) o sin asalto (no se presenta actos de intimidación) a domicilios en el DMQ desde el 2011 hasta el 2013.

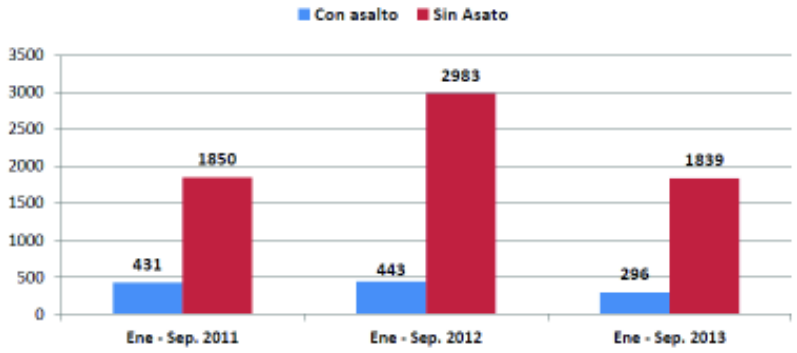

Figura 2.1 Denuncias de robos residenciales anuales [47]

Los robos en hogares a partir del 2013 se reducen en un 24% con respecto al año anterior. Los meses que se presentan mayores denuncias ocurren el periodo de vacaciones escolares, agosto y septiembre. Debido a esta problemática de inseguridad ciudadana, el Municipio impulsó los sistemas de alarmas residenciales principalmente en la zona Norte-Centro, como medida para disminuir la delincuencia en la comunidad, fortalecer el vínculo de la comunidad y la policía.

Según los datos presentados en la figura 2.2, tomados del informe del OMSC en el periodo de enero a septiembre del 2013, se han presentado mayores denuncias de robos en la tarde y entre semana, principalmente los días jueves.

Figura 2.2 Ocurrencia de robos residenciales semanales [47]

Además, las alarmas comunitarias actuales tienen el problema del poco incentivo de sus miembros a cooperar en la seguridad de la colectividad. Por otro lado, la necesidad de contar con un sistema de seguridad, muchas veces implica un alto costo anual. Generalmente, el dueño de la vivienda contrata a una empresa que se encarga del monitoreo y protección, así como, de la implementación de una infraestructura que conlleva las alarmas instaladas en las casas [48].

Actualmente, en el mercado local existen varias empresas que brindan el servicio de instalación, mantenimiento y monitoreo del sistema de alarmas. Por lo general, muchas veces los eventos (robo, intrusión, incendio) que se generan desde el panel de alarma convencionales en los hogares son recibidos en las Centrales de Monitoreo que prestan este servicio vía PSTN (Public Switched Telephone Network), donde llega la información de los usuarios. De esta manera, la línea telefónica permite que el sistema de alarma este directamente comunicado con la central.

La eficiencia de estos sistemas depende de la estación centralizada, su ubicación física, número de usuarios, zona de activación y tiempo de respuesta. Según la Asociación Latinoamericana de seguridad existe mayor probabilidad que se produzca un robo en hogares que no cuentan con un sistema de alarmas. Estadísticamente, las viviendas de construcción moderna, hogares con lotes baldíos presentan el doble de probabilidad de ser víctimas de un robo [49].

Por lo general, las empresas de seguridad instalan el sistema de alarma con sensores o detectores en puertas y ventanas. Las señales se transmiten hacia el panel y de este hacia el receptor que está conectado a la Central de monitoreo, la cual gestiona y comprueba toda la información. Las empresas proporcionan un servicio de monitoreo continuo los 365 días del año. Cuando se produce un evento de emergencia y no tiene respuesta por parte de alguna persona de la vivienda o no se da la clave correcta, activan el protocolo de seguridad. De esta forma, se envía al personal de vigilancia, se notifica a la policía o se alerta a los bomberos dependiendo de la respuesta correspondiente.

Requerimientos para el sistema de alarmas residenciales utilizando la Tecnología *Blockchain*

Los requerimientos para el nuevo sistema de alarmas residenciales teniendo presente la Tecnología de *Blockchain*, cadena de bloques, parten de la misma distribución y diseño de espacios de las 30 casas tipo del sistema de alarma tradicional. Para este criterio se considera la norma NFPA[34] 72, pero con las siguientes especificaciones:

- Las 30 casas de construcción moderna necesitan del sistema de alarmas y monitoreo 24/7, sin necesidad de contratar a una empresa que provea este servicio, pero con la confianza que la información del sistema va a permanecer protegida y ningún usuario de las 30 casas va a poder manipular los datos.
- Al no contar con una empresa que realice el monitoreo del sistema de alarmas, el control de los eventos deber ser permanente, es decir detectar oportunamente el auxilio con un tiempo de respuesta casi inmediato.
- Todas las casas cuentan con servicio de Internet y su computador personal de escritorio, lo que va a permitir de una manera fácil y eficiente implementar la nueva tecnología *Blockchain*. Adicionalmente se requiere un dispositivo para interactuar con los eventos y el sistema descentralizado.
- Se asume que la comunidad desea contribuir dinámicamente en la seguridad de la colectividad por medio del consenso de los eventos generados en el sistema de alarmas, evitando de esta forma depender de algún intermediario o entidad centralizada.
- Comunicación transparente entre los miembros de la comunidad y la UPC, donde este organismo sabrá inmediatamente que ocurre un evento de emergencia directamente, cooperando como parte de la comunidad, sin recibir ninguna llamada de la empresa de monitoreo.
- El mantenimiento y monitoreo de la gestión de los eventos de alarma será descentralizado y de forma independiente, donde cada usuario de las 30 casas cuando desee, puede visualizar su información y saber qué pasa con el resto de la comunidad, de forma transparente y confiable, sin necesidad de contratar a algún intermediario.

[34] NFPA (*National Fire Protection Association*): La Asociación Nacional de Protección contra Incendio, menciona las normas para el sistema de seguridad con respecto a su diseño, recomendaciones y montaje de la comunicación de las alarmas a la central de monitoreo.

2.2. Fase de gestión de los eventos

Sistema de alarmas residenciales Centralizado

Se considera una casa de construcción moderna de tres niveles para implementar un sencillo sistema de alarmas sin considerar un CCTV. Cabe indicar que el mismo criterio de distribución del número de sensores se puede utilizar para una estructura diferente; es decir, para una casa de 2 pisos o para una sola planta, donde se conserve todos los ambientes que se van a detallar a continuación.

Considerando las especificaciones mínimas de la norma NFPA 72 en el perímetro de la planta baja se separa por zonas de acuerdo a la distribución del espacio. La figura 2.3 muestra únicamente esta planta de la casa tipo, que está cubierta por contactos magnéticos que conforman la Zona 1.

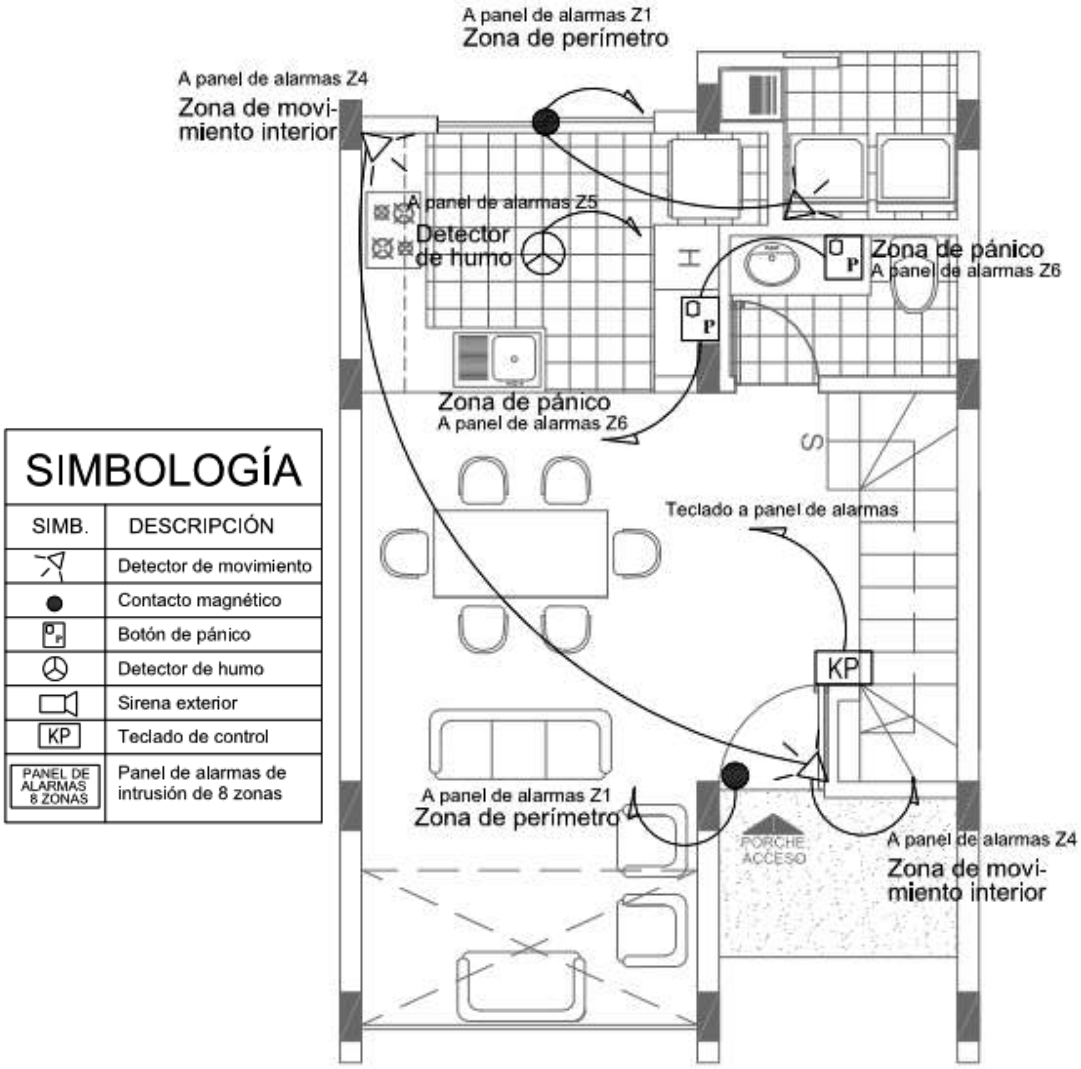

Figura 2.3 Distribución de puntos de la Planta Baja.

La cocina cuenta con un detector de humo, que forma parte de la Zona 5; en esta misma zona podría utilizarse otro tipo de sensores, por ejemplo, el Gas Licuado de Petróleo, GLP. Para la distribución de los detectores de humo se toma como criterio las recomendaciones de instalación de la normativa CAN/ULC-S553-M86 para viviendas. Los sensores de movimiento en planta baja se colocan para delimitar la Zona 4. El botón de pánico se ubica en un lugar estratégico de la cocina y pertenece a la Zona 6.

La figura 2.4 indica la distribución de puntos de la primera planta alta. En esta área existe un contacto magnético para el ingreso del balcón, que pertenece a la Zona 2; un sensor de movimiento que cubre el pasillo y corresponde a la Zona 4. El botón de pánico se coloca en un punto estratégico del baño, para la Zona 6. Generalmente, los baños son la ubicación utilizada para este tipo de dispositivo. El panel de alarmas, se ubica en esta planta, en un lugar céntrico donde el cliente tenga un fácil acceso.

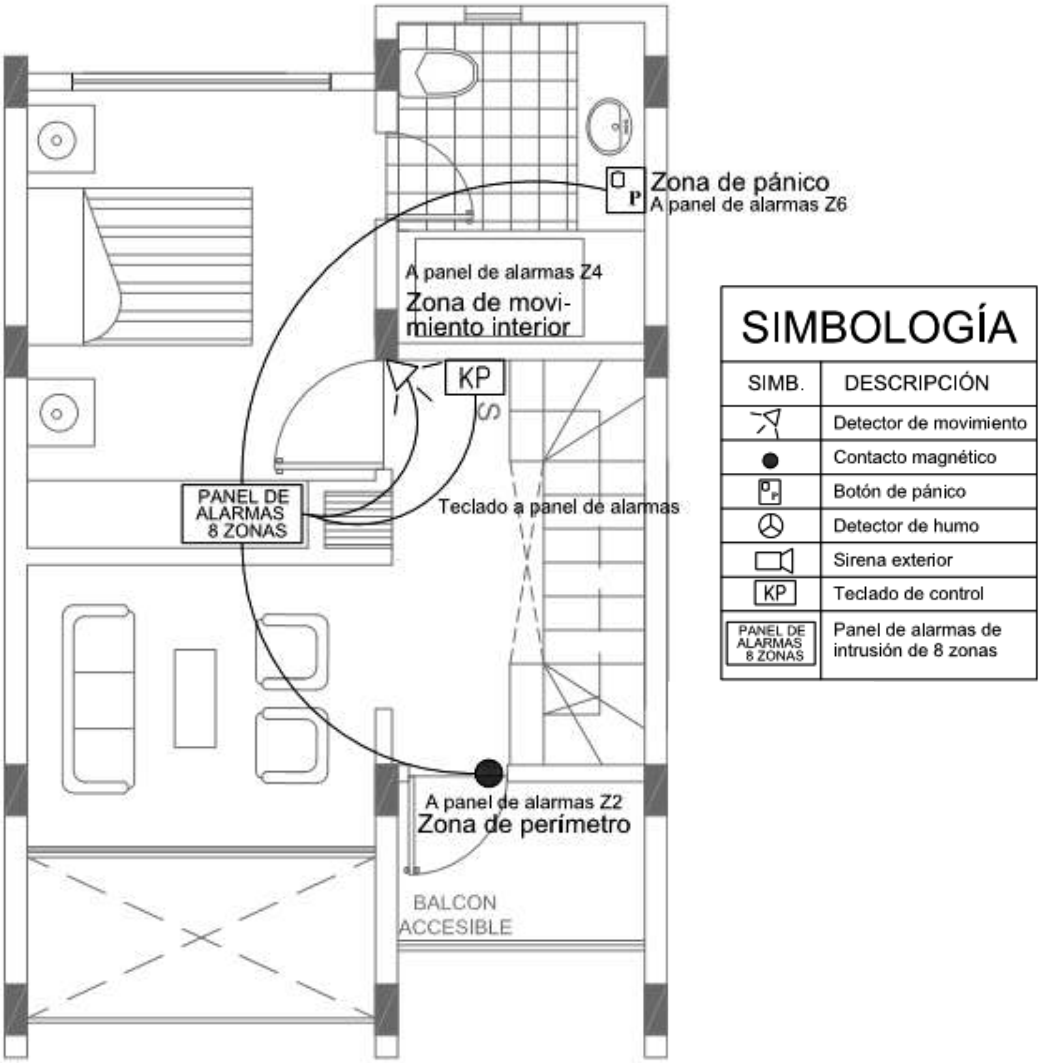

Figura 2.4 Distribución de puntos de la Primera planta.

Los puntos de distribución de la segunda planta alta, se indican en la figura 2.5. Se analiza el posible punto de ingreso, por la terraza accesible que está cubierto por la Zona 3 mediante un contacto magnético. La Zona 6, contiene el botón de pánico, ubicado en el baño. La Zona 4, está cubierta por un detector de movimiento.

En este piso en la parte exterior, se coloca una sirena que va directamente conectada al panel de alarmas. Esta se activa en caso de emergencia, si un dispositivo de seguridad detecta una intrusión.

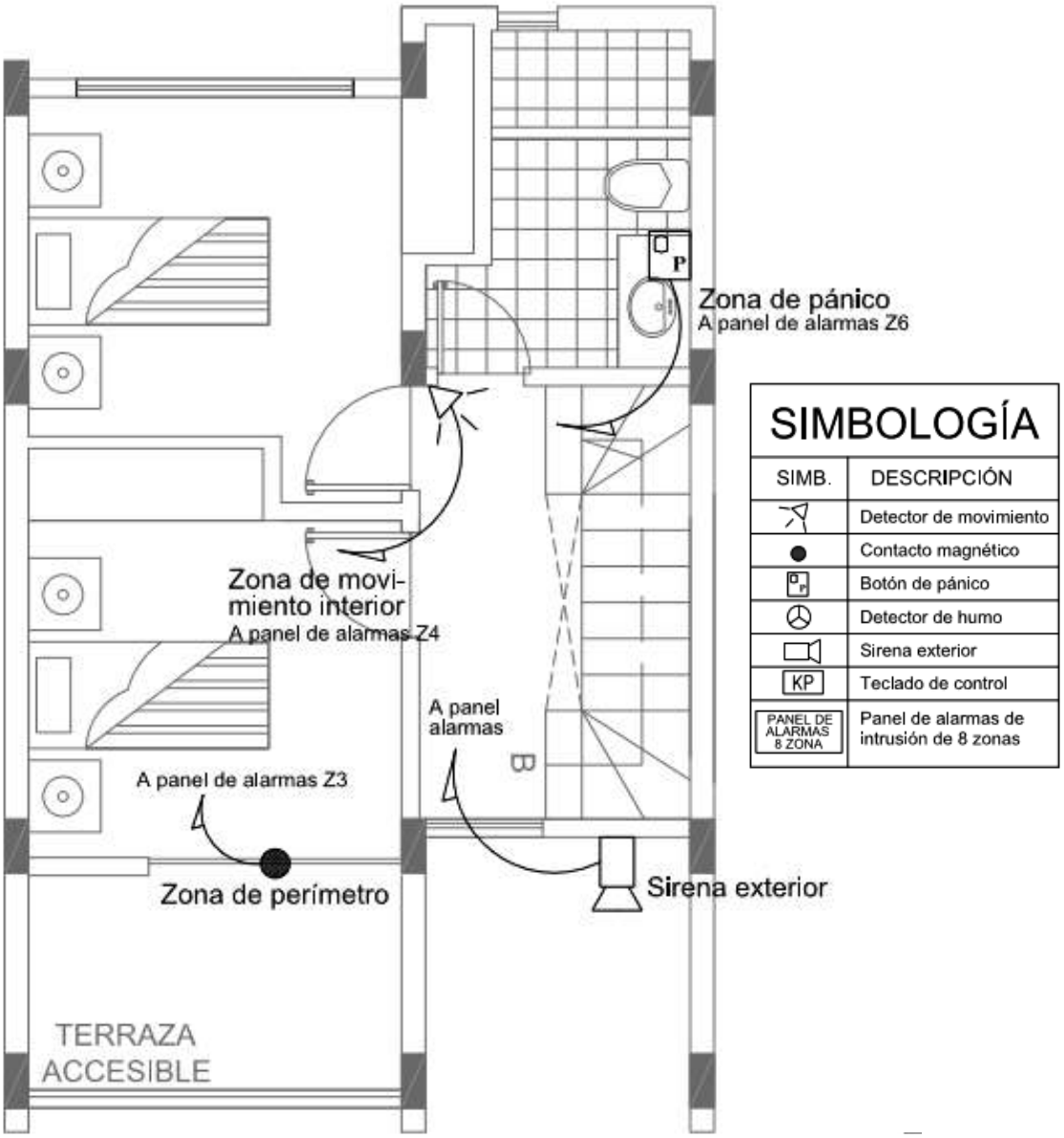

Figura 2.5 Distribución de puntos de la Segunda planta.

Los sensores de movimiento en todos los pisos forman parte de la zona 4. Si bien es conveniente separar las zonas por áreas, en este caso específico es preferible utilizar una sola zona pues en caso de armado en presencia (nocturno), la única zona que no produciría alarma durante la noche es la zona 4. Esto permite ahorrar el número de zonas a utilizarse para el panel de alarmas. Todas las zonas deben estar configuradas de acuerdo al tipo de sensor que contienen, especialmente las zonas 5 y 6 que deben activarse independientemente de que el sistema este armado o desarmado.

Se dispondrán de dos teclados para la operación del panel de alarmas, uno cercano a la puerta principal en la planta baja y otro en el área de dormitorio en la primera planta. Se consideran dos teclados pensando en su uso a la entrada/salida del domicilio y al armado nocturno como se muestra en las figuras 2.3 y 2.4.

Por lo expuesto anteriormente, se determina que el número de zonas mínimo para el panel de alarmas es de 6, pero se selecciona un panel de 8 zonas considerando dos zonas de reserva para uso futuro. El panel debe tener capacidad para transmitir eventos en formato Contact ID[35] para su monitoreo, es obligatorio que disponga de terminales de conexión *TIP and RING,* de esta forma la comunicación con la empresa de monitoreo, se realice de forma habitual a través de la línea telefónica.

Los componentes fundamentales del sistema de alarma son los detectores de movimiento y el detector de humo, que requieren alimentación eléctrica; en cambio, los botones y contactos magnéticos son los elementos pasivos. Todos estos sensores sirven para detectar una intrusión y se conectan al panel, donde los eventos son enviados hacia la central receptora a través de la PSTN. La empresa de seguridad se encarga de realizar el monitoreo remoto y seguimiento permanente de los eventos, ya sea en activación o desactivación de las alarmas. Si surge una alerta en el sistema, se activa la alarma y sirena, la operadora del este servicio se encarga de contactarse con el propietario y la policía.

La tabla 2.1 indica el equipamiento de los dispositivos electrónicos, que se consideran necesarios para la instalación del sistema de alarmas. Los elementos pasivos comprenden el conjunto de tubería, accesorios y material en general, van a ser los puntos tipo A. Los equipos que requieren alimentación eléctrica, son de tipo B. Adicionalmente se trabajará con los puntos para el panel de alarma, teclado, y sirena exterior.

[35] ContactID es una secuencia de tonos DTMF que envía el panel de alarma, agrupados en un determinado orden, para que la central de monitoreo identifique el evento. El panel de alarmas realiza una llamada telefónica a la central y le informa de los eventos mediante pulsaciones a una frecuencia definida por el estándar.

Tabla 2.1 Equipamiento para el sistema de alarmas.

	Planta Baja	1era Planta Alta	2da Planta Alta	Total de Puntos
Punto para Alarma Tipo A	4	1	1	6
Punto para Alarma Tipo B	4	2	2	8
Punto para panel de alarmas	0	1	0	1
Punto para teclado	1	1	0	2
Punto para sirena	0	0	1	1
Sensor de movimiento	3	1	1	5
Detector de humo	1	0	0	1
Botón de pánico	2	1	1	4
Contacto magnético	2	1	1	4
Teclado de control	1	1	0	2
Panel de alarmas	0	1	0	1
Sirena exterior	0	0	1	1

Un detector de movimiento típico, el LC-100 de la marca DSC, tiene un consumo de 10mA en activo y 8mA en espera, como se indica en las especificaciones técnicas del Anexo II. Tomando como referencia el Anexo III, se detalla el detector de humo D732 de marca Bosch, cuyo consumo máximo es de 18mA.

Referencialmente se toma en cuenta el panel de alarmas comercial PC1832, que es ampliamente usado en el mercado, tiene una fuente auxiliar de 700mA en su propia tarjeta; las especificaciones técnicas se encuentran en el Anexo IV. La tabla 2.2 indica los datos de consumo y las cantidades de elementos que resultaron de la distribución de los sensores del sistema de alarmas, con 68mA claramente se puede afirmar que el panel de alarmas no necesita fuentes adicionales.

Tabla 2.2 Consumo de energía de los dispositivos conectados a la fuente auxiliar.

Elementos	Número de Puntos	Consumo (mA)	Consumo Total (mA)
Sensor de Movimiento	5	10	50
Detector de Humo	1	18	18
			68

Sistema de Alarmas Residenciales utilizando la Tecnología *Blockchain*

En este caso, el sistema de alarmas basado con la tecnología *Blockchain* va a mantener el mismo criterio de los puntos de distribución del sistema de alarmas tradicional, dentro de cada casa de tres niveles, donde se reutilizarán los mismos equipos anteriormente expuestos. La tecnología *Blockchain* sustituye la central receptora y trabaja directamente con las señales generadas del panel de alarmas, por medio de sus salidas programables. Por lo tanto, la gestión de la información de los eventos se realiza sobre Internet, mediante un sistema descentralizado, sin necesidad de contratar a intermediarios para realizar la gestión de los eventos y el monitoreo del sistema.

El principio de la tecnología *Blockchain* privada, considerando la plataforma de *Ethereum* trabaja en un ambiente *peer-to-peer*, que está conformada nodos y mineros. Cada casa va a requerir un Raspberry Pi, *RPI*, para ser un nodo y se va a necesitar cuatro mineros ubicados en la UPC más cercana y el resto en cualquier vivienda de las 30 casas. Se piensa en 4 mineros dentro de la comunidad para garantizar una mayor confiabilidad y transparencia del servicio. Los mineros van a estar presentes en la red por medio de computadores personales. Todos los nodos van a ejecutar el mismo protocolo de consenso.

Cabe indicar que para la sincronización de los eventos en toda la red P2P, el sistema descentralizado necesita mínimo dos mineros para funcionar [50], pero para evitar que algunas transacciones no sean recibidas o procesadas si se cae uno de los dos mineros, se considera cuatro mineros como respaldo en la red, para garantizar y mantener la sincronización de la información entre los nodos de la red.

En la plataforma de *Ethererum*, el contrato inteligente permite ejecutar automáticamente el monitoreo del sistema en cada nodo de las 30 casas, los eventos de alarma generan una transacción, que se van a ser registras en la cadena de bloques de forma pública. La ejecución del contrato requiere un pago por este servicio en *tokens*.

Si se produce una intrusión en el sistema, el tiempo respuesta de la red será en segundos, donde la responsabilidad de la seguridad está distribuida en toda la comunidad. Los propios vecinos participan voluntariamente para enfrentar los problemas individuales de inseguridad a nivel colectivo. La policía comunitaria, UPC, está al tanto si ocurre un evento de emergencia ya que es miembro de la red y tiene una estrecha relación con la ciudadanía. Todo este proceso, fomenta una cultura de colaboración comunitaria, con vecinos comprometidos en su propio bienestar.

La tabla 2.3 indica los requisitos mínimos de hardware para implementar el nodo de la red privada en *Ethereum.*

Tabla 2.3 Requisitos de hardware para el nodo en la red *Ethereum* [51].

Equipo	Características
Raspberry Pi	Versión 3. Procesador ARM. 4 núcleos a 1.2 GHz de 64 bits. 1 GB de RAM. Video, Salida HDMI, Ethernet, Wi-Fi 802.11 b/g/n, Bluetooth 4.1 y 4 puertos USB y slot para microSD.
Fuente de alimentación	Cargador con salida micro USB de 2A.
Dispositivos de salida	• Pantalla LCD, monitor o Televisión con salida HDMI. • Teclado • Mouse
Tarjeta Micro SD	Mayor a 8GB mínimo de clase 10.
Disipador de calor	2 disipadores de calor

Se pega el adhesivo de los dos disipadores de calor en la parte superior de la placa del Raspberry, uno en su procesador y el otro en la controladora de red, como se muestra en la figura 2.6.

Figura 2.6 *Raspberry Pi* y disipadores de calor

La figura 2.7 indica los elementos que forman parte del hardware necesario para levantar el nodo de la red *Ethereum*. Se trabaja con una tarjeta micro SD de 16GB, una pantalla LCD de 5” o cualquier monitor disponible, una fuente de alimentación de 5V, teclado, mouse y por supuesto el *Raspberry Pi*.

Figura 2.7 Hardware para implementar el nodo

En la tarjeta microSD se instala el sistema operativo Rasbian[36] para que arranque el Raspberry. Debido a las limitaciones de hardware, el Raspberry Pi no se puede usar para implementar algún minero, es decir, el RPI no puede crear nuevos bloques en las transacciones de la red.

Para este estudio, no se va a implementar directamente el nodo en un computador personal, ya que es necesario adquirir un hardware adicional en la PC para controlar las salidas programables, PGM, del panel de alarmas. El RPI soluciona este inconveniente, como especifica la figura 2.8. Mediante la distribución de pines se puede trabajar con los pines GPIO[37] para controlar los eventos de alarma, sirena y el botón de pánico.

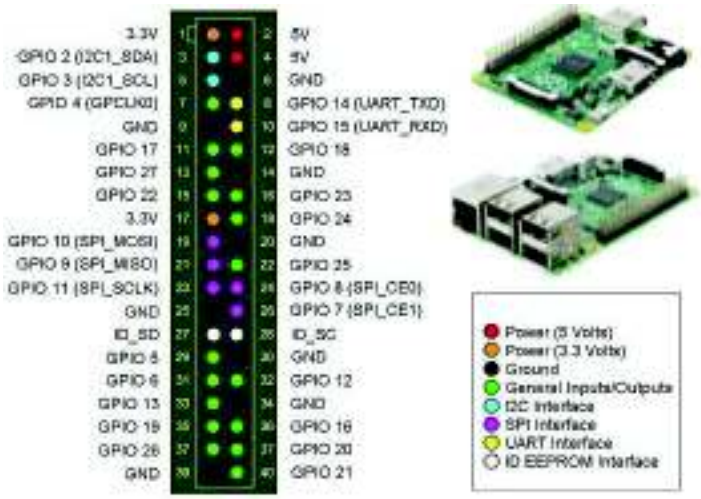

Figura 2.8 Distribución de pines del Raspberry PI3 [52]

[36] Rasbian es el sistema operativo de Linux y está basado en la distribución de Debian.
[37] GPIO (*General Purpose Input/Output*) pin que permite configurar las entradas y salidas de propósito general del RPI.

Para implementar el minero, como ya se mencionó antes, es preferible no usar un Raspberry Pi ya que demanda muchos recursos, tiempo y potencia de procesamiento. El hardware adecuado para implementar un minero es una GPU, ya que se aprovecha al máximo su potencial de procesamiento. En este caso de estudio del sistema de alarmas de 30 casas, como no demanda tremenda dificultad como los sistemas financieros se considera un computador convencional para trabajar como minero.

La tabla 2.4 indica los requerimientos mínimos necesarios para el computador convencional funcioné como minero.

Tabla 2.4 Requisitos de hardware para el minero en la red *Ethereum* [53].

Sistema	Características
Procesador	Intel Core/Celeron de 2.8Ghz 6ta o 7ma generación.
Memoria RAM	4GB
Interfaz de la memoria	DDR4 2400MT/s
Motherboard	LGA1151/Intel H110

Para este trabajo, se va a considerar la red privada *Ethereum*. El objetivo es evitar conectarse a la *Main Network*, para no cargar todo el *ledger* existente en el sistema descentralizado. Este proceso demanda la sincronización de toda la base de datos con al menos 2GB de memoria, lo que requiere un hardware adicional como el GPU. La figura 2.9 indica las 62.619.154[38] transacciones de *Blockchain*, que se incrementan cada día en función de la demanda de bloques. El Anexo V, muestra mayores detalles de las transacciones de *Blockchain*.

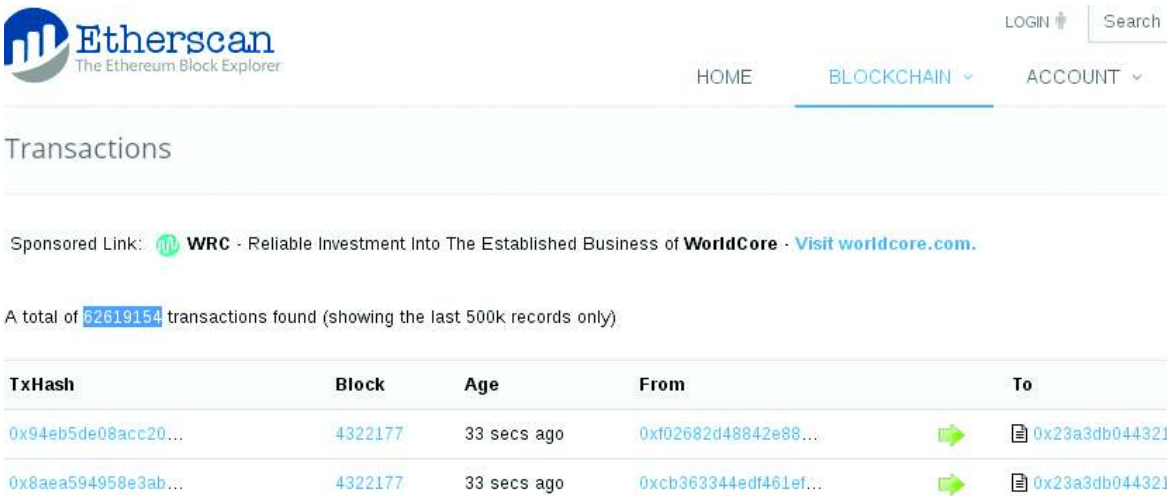

Figura 2.9 Número de transacciones de *Blockchain* en la red pública

[38] Valor tomando de la página oficial de *Blockchain* https://etherscan.io el 29 de Septiembre, 2017 a las 10h32

Blockchain con base a la Plataforma de *Ethereum*

La figura 2.10 muestra la red privada *Ethereum* de las 30 casas que estaría presente a través de nodos, *Raspberry Pi* 3, y 4PCs para los mineros, donde se garantiza la confiabilidad de la red y no exista una degradación en el rendimiento de la misma, por lo tanto, si llega a fallar algún minero, la calidad de la transacción de los eventos será respaldada por el resto de mineros. Todos los nodos van a estar sujetos bajo los mismos principios de la tecnología *Blockchain* y se ejecutarán automáticamente con la ayudad del contrato inteligente sin necesidad de terceros. Si se analiza el minero 2, se observa que se propaga el bloque hacia sus nodos vecinos.

Las salidas programables del panel de alarma de cada casa van conectadas a las entradas GPIO del RPI. El RPI está interconectado con todos los nodos de la red *Ethereum* privada a través de Internet. Existe un minero en el UPC para que pueda asistir inmediatamente si se produce un evento de emergencia, los tres mineros restantes se pueden configurar en cualquiera de las casas.

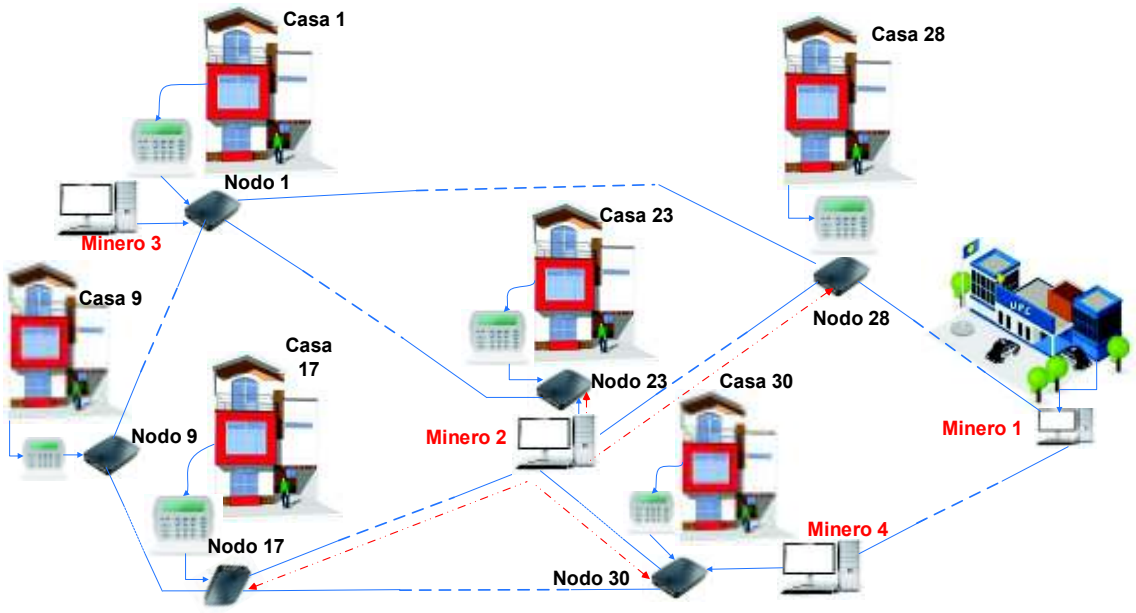

Figura 2.10 Red *Ethereum* privada de las 30 casas.

Se van a mencionar los pasos para configurar un nodo y un minero, después el proceso se repite para el resto de nodos y mineros que faltan, con el fin de formar la red P2P privada con los mismos principios que la Red principal de *Ethereum, Main Network,* y algoritmo de consenso, pero limitando el acceso de la información de la red.

Nodo con Raspberry Pi (RPi).

Antes de proceder a instalar el nodo en Raspberry Pi, se realizará una configuración previa en el *Configure advanced settings*:

- Cambiar el *hostname,* por el nombre del nodo de la red, mediante el comando sudo raspi-config. En este caso se usa como nomenclatura **SisAlarmasNodo1.**
- Después, se procede a configurar la interfaz Wi-fi en el archivo wpa_supplicant.conf, en el ssid se escribe el nombre de la red y en psk la contraseña.

Ahora en forma práctica se va a configurar en el nodo en Raspberry Pi considerando los siguientes pasos:

- Lo primero es saber las características del procesador y versión del RPi, usando el comando cat/proc/cpuinfo como se muestra en la figura 2.11.

```
pi@SistAlarmasNodo1: ~
File  Edit  Tabs  Help
pi@SistAlarmasNodo1:~ $ cat /proc/cpuinfo
processor       : 0
model name      : ARMv7 Processor rev 4 (v7l)
BogoMIPS        : 38.40
Features        : half thumb fastmult vfp edsp neon vfpv3 tls vfpv4 idiva idivt
vfpd32 lpae evtstrm crc32
CPU implementer : 0x41
CPU architecture: 7
CPU variant     : 0x0
CPU part        : 0xd03
CPU revision    : 4

processor       : 1
model name      : ARMv7 Processor rev 4 (v7l)
BogoMIPS        : 38.40
Features        : half thumb fastmult vfp edsp neon vfpv3 tls vfpv4 idiva idivt
vfpd32 lpae evtstrm crc32
CPU implementer : 0x41
CPU architecture: 7
CPU variant     : 0x0
CPU part        : 0xd03
CPU revision    : 4
```

Figura 2.11 Características del procesador y versión del RPI.

- Luego se ingresa a la página oficial de *Go-Ethereum* https://geth.ethereum.org/downloads/ y se busca el Geth[39] de acuerdo al modelo del RPi. En este caso el modelo es ARMv7 y la última versión oficial del Geth es 1.8.1 como se indica en la figura 2.12.

[39] *Geth* es el sistema operativo para la implementación de *Go-Ethereum*

```
pi@SistAlarmasNodo1: ~/geth-linux-arm7-1.8.1-1e67410e
File  Edit  Tabs  Help
pi@SistAlarmasNodo1:~ $ wget https://gethstore.blob.core.windows.net/builds/geth
-linux-arm7-1.8.1-1e67410e.tar.gz
--2018-06-07 08:34:47--  https://gethstore.blob.core.windows.net/builds/geth-lin
ux-arm7-1.8.1-1e67410e.tar.gz
Resolving gethstore.blob.core.windows.net (gethstore.blob.core.windows.net)... 4
0.113.27.176
Connecting to gethstore.blob.core.windows.net (gethstore.blob.core.windows.net)|
40.113.27.176|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10428054 (9.9M) [application/octet-stream]
Saving to: 'geth-linux-arm7-1.8.1-1e67410e.tar.gz.1'

geth-linux-arm7-1.8 100%[===================>]   9.94M  1.26MB/s   in 8.4s

2018-06-07 08:34:57 (1.18 MB/s) - 'geth-linux-arm7-1.8.1-1e67410e.tar.gz.1' save
d [10428054/10428054]
```

Figura 2.12 Instalación del Geth en RPI.

- La figura 2.13 indica cómo se extrae ese archivo en el RPi y se copia el geth en la carpeta /usr/local/bin

```
pi@SistAlarmasNodo1: ~/geth-linux-arm7-1.8.1-1e67410e
File  Edit  Tabs  Help

pi@SistAlarmasNodo1:~ $ tar zxvf geth-linux-arm7-1.8.1-1e67410e.tar.gz
geth-linux-arm7-1.8.1-1e67410e/
geth-linux-arm7-1.8.1-1e67410e/COPYING
geth-linux-arm7-1.8.1-1e67410e/geth
pi@SistAlarmasNodo1:~ $ cd geth-linux-arm7-1.8.1-1e67410e
```

Figura 2.13 Extracción del archivo geth.

- Para verificar si se instaló correctamente el archivo Geth y su versión se usa el comando geth *version*, ver figura 2.14.

```
pi@SistAlarmasNodo1:~/geth-linux-arm7-1.8.1-1e67410e $ geth version
Geth
Version: 1.8.1-stable
Git Commit: 1e67410e88d2685bc54611a7c9f75c327b553ccc
Architecture: arm
Protocol Versions: [63 62]
Network Id: 1
Go Version: go1.9.4
Operating System: linux
GOPATH=
GOROOT=/usr/local/go
```

Figura 2.14 Comprobación de la instalación del archivo Geth

- La figura 2.15 indica cómo se inicia el servicio de *Ethereum*, se usa el comando geth. Ahora el nodo ya se puede sincronizar a la cadena de la red principal, *Main Network*, pero este proceso puede tomar varios días. Para terminar el proceso se presiona las teclas CTRL+C.

Se procede a seguir los pasos anteriores, para crear el resto de nodos de la red P2P.

```
pi@SistAlarmasNodo1: ~/geth-linux-arm7-1.8.1-1e67410e
File  Edit  Tabs  Help
pi@SistAlarmasNodo1:~/geth-linux-arm7-1.8.1-1e67410e $ geth
INFO [06-07|08:38:03] Maximum peer count                       ETH=25 LES=0 tota
l=25
INFO [06-07|08:38:03] Starting peer-to-peer node               instance=Geth/v1.
8.1-stable-1e67410e/linux-arm/go1.9.4
INFO [06-07|08:38:03] Allocated cache and file handles         database=/home/pi
/.ethereum/geth/chaindata cache=768 handles=1024
INFO [06-07|08:38:46] Initialised chain configuration          config="{ChainID:
 1 Homestead: 1150000 DAO: 1920000 DAOSupport: true EIP150: 2463000 EIP155: 2675
000 EIP158: 2675000 Byzantium: 4370000 Engine: ethash}"
INFO [06-07|08:38:46] Disk storage enabled for ethash caches   dir=/home/pi/.eth
ereum/geth/ethash count=3
INFO [06-07|08:38:46] Disk storage enabled for ethash DAGs     dir=/home/pi/.eth
ash                count=2
INFO [06-07|08:38:46] Initialising Ethereum protocol           versions="[63 62]
" network=1
INFO [06-07|08:38:46] Loaded most recent local header          number=149498 has
h=dcc75e…8ec2f3 td=407372464445835002
INFO [06-07|08:38:46] Loaded most recent local full block      number=0      has
h=d4e567…cb8fa3 td=17179869184
INFO [06-07|08:38:46] Loaded most recent local fast block      number=146676 has
```

Figura 2.15 Iniciando el nodo de *Ethereum* en RPI

Minero en el Computador

Al momento de trabajar con el computador es necesario saber el sistema operativo que se va a implementar, sea Linux, Windows o Mac. Dependiendo de esta plataforma varía la instalación. En este caso, se va a utilizar Linux, con la versión de Ubuntu se simulará el minero en la red de *Ethereum.*

El minero permitirá validar y propagar el bloque dentro de la *Blockchain*. Específicamente, el minero generará el *token (Ether*) en *Ethereum* para procesar la transacción en esta red privada.

Para mantener la sincronización entre los datos es necesario al menos implementar dos mineros. Al tener un sólo un minero, se corre el riesgo que algunas transacciones no sean procesadas y podrían quedarse pendientes. Al trabajar con dos mineros este problema se solventaría y tendría sentido el algoritmo de consenso.

La figura 2.16 especifica el proceso para crear los mineros en la red privada y toma en cuenta los siguientes procesos [54]:

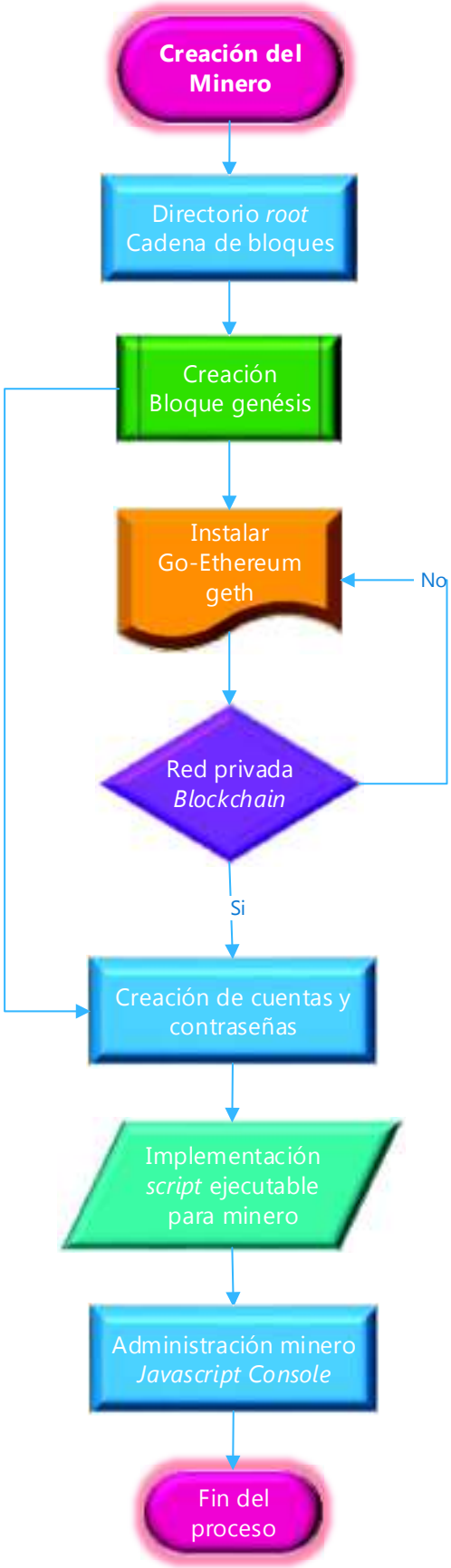

Figura 2.16 Diagrama de creación de minero

- Lo primero es identificar el nombre del minero en el computador con el comando gedit /etc/*hostname*. Se trabaja con el identificador **SisAlarmasMinero**.

- Luego, se crea el directorio principal o *root,* donde van a correr todos los mineros y deben estar en la misma ubicación. La carpeta *ChainSkills* van a almacenar los dos mineros. Para crear la carpeta de los mineros se usa el comando mkdir –p ~/ChainSkills/nombre de los mineros.

- Para crear una cadena de bloques privada, se instala el bloque génesis. Este bloque es el punto de partida o *root* de la cadena de bloques, desde donde se va a construir toda la *blockchain* y define las condiciones para que los nodos se unan a la red e indica la dificultad de la transacción que va a ser procesada.

- Primero, se procede a crear el bloque génesis de cada minero. La figura 2.17 indica el contenido del archivo genesis.json, que se encuentra el directorio principal de la cadena de bloques, *ChainSkills*. Tiene los siguientes parámetros (en hexadecimal) en la cabecera del bloque génesis [40]:

    - *Nonce*: hash[40] de 64 bits que combinado con *mixhash* sirve para calcular la *PoW*. En la cabecera del bloque génesis se usa el *nonce* que va a servir para que el algoritmo criptográfico realice la prueba de trabajo.

    - *Mixhash*: hash de 256 bits que combinado con *nonce* sirve para calcular la *PoW*. Sirve para comprobar que el bloque ha sido extraído correctamente, en este caso es **0**. Además, indica que el minero gasta esfuerzo computación por realizar la prueba de trabajo.

    - *Difficulty*: valor escalar de 32 bits, indica el nivel de dificultad para minar el bloque [15]. Mientras mayor sea su valor, más complejo son los cálculos estadísticos que realizará el minero. En este caso del sistema de alarmas, se considera que los eventos requieren una acción inmediata por lo tanto se requiere un menor tiempo de generación de los bloques, por esta razón se considera un nivel de dificultad bajo para realizar el proceso de descubrimiento del bloque válido.

    - *Alloc*: permite manejar los *Ethers* dentro de los *wallets* en la red *Ethereum*.

[40] hash es la huella digital del bloque, se encuentra en la cabecera e identifica un bloque de forma única e inequívoca y se origina independiente por cualquier nodo de la red.

- *Coinbase*: dirección de 160 bits, donde se van a transferir las recompensas, *Ethers*, del proceso de minería exitoso. Al crear el bloque génesis no se asigna ningún tipo de reembolso ya que los bloques siguientes recién van a crear un nuevo bloque y si se va a producir el proceso de minería.

- *Timestamp*: valor escalar que permite identificar el orden del bloque dentro de la *blockchain*. Como el bloque génesis es el primer bloque desde donde va a partir la cadena no requiere un tiempo inicial se deja en cero. El *timestamp*, marca de tiempo, tiene una relación inversa con la dificultad, es decir que mientras mayor sea el valor del *timestamp*, menor será el valor de la dificultad y el tiempo esperado para generar siguiente bloque.

- *ParentHash*: hash de 256 bits, apunta hacia el bloque padre, es decir cada bloque contiene el hash de su padre dentro de su propia cabecera. El bloque génesis es el punto de partida de toda la cada de bloques, no hace referencia a ningún bloque anterior, su valor es de cero.

- *ExtraData:* contiene datos relevantes del bloque con una capacidad de 32 bytes. En este caso se ha colocado **Bloque Genesis-SistAlarmas**

- *Gaslimit:* valor escalar que indica el límite del consumo de Gas por bloque del Contrato que se puede usar en la cadena.

- *Config:* configuración adicional para describir la cadena de bloque. Donde se coloca la identificación de la cadena, *chainId*, el motor de consenso, *homesteadBlock*[41] y los números de los bloques eip[42] [55].


```
{
 "nonce": "0x0000000000000042",
 "mixhash": "0x0000000000000000000000000000000000000000000000000000000000000000",
 "difficulty": "0x400",
 "alloc": {},
 "coinbase": "0x0000000000000000000000000000000000000000",
 "timestamp": "0x00",
 "parentHash": "0x0000000000000000000000000000000000000000000000000000000000000000",
 "extraData": "0x426c0f7175652047656e65736973732d53697374416c61726d6173",
 "gasLimit": "0xffffffff",
 "config": {
    "chainId": 42,
    "homesteadBlock": 0,
    "eip155Block": 0,
    "eip158Block": 0
        }
}
```


Figura 2.17 Archivo del Bloque Génesis

[41] Homestead es la segunda versión que lanzó *Ethereum* en 2016, que incluye protocolos y actualizaciones de la red [62].
[42] EIP, *Ethereum Improvement Proposals*, son las Propuestas de mejora de *Ethereum* que describes los estándares para la plataforma y del contrato.

- Se procede a implementar *Go Ethereum, Geth,* que es la interfaz de comandos en línea (*Command Line Interface*, CLI) para correr los nodos de *Ethereum* [56].

  La figura 2.18 indica los paquetes que se instalan para correr geth, en el repositorio PPA[43]. Primero, se instala las propiedades del paquete, después se habilita el repositorio donde va a correr *Go-Ethereum*, luego se actualiza la lista de paquetes y versiones disponibles en el repositorio.

```
alexita@SisAlarmasMinero: ~
alexita@SisAlarmasMinero:~$ sudo apt-get install software-properties-common
Reading package lists... Done
Building dependency tree
Reading state information... Done
software-properties-common is already the newest version (0.96.20.7).
0 upgraded, 0 newly installed, 0 to remove and 121 not upgraded.
alexita@SisAlarmasMinero:~$ sudo add-apt-repository -y ppa:ethereum/ethereum
gpg: keyring `/tmp/tmpveezp9nq/secring.gpg' created
gpg: keyring `/tmp/tmpveezp9nq/pubring.gpg' created
gpg: requesting key 923F6CA9 from hkp server keyserver.ubuntu.com
gpg: /tmp/tmpveezp9nq/trustdb.gpg: trustdb created
gpg: key 923F6CA9: public key "Launchpad PPA for Ethereum" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
OK
alexita@SisAlarmasMinero:~$ sudo apt-get update
Hit:1 http://us.archive.ubuntu.com/ubuntu xenial InRelease
Get:2 http://security.ubuntu.com/ubuntu xenial-security InRelease [107 kB]
Get:3 http://ppa.launchpad.net/ethereum/ethereum/ubuntu xenial InRelease [17.5
 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu xenial-updates InRelease [109 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease [107 kB]
Get:6 http://ppa.launchpad.net/ethereum/ethereum/ubuntu xenial/main i386 Packa
ges [6,692 B]
Get:7 http://us.archive.ubuntu.com/ubuntu xenial-updates/main i386 DEP-11 Meta
data [318 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu xenial-updates/main DEP-11 64x64 Ico
ns [224 kB]
Get:9 http://ppa.launchpad.net/ethereum/ethereum/ubuntu xenial/main Translatio
n-en [3,072 B]
```

Figura 2.18 Instalación de los repositorios de Geth

En cambio, la figura 2.19 muestra como instalar la dependencia de geth y para comprobar que este paquete está instalado correctamente se usa el comando *geth version*, que indica las características principales como son la versión, arquitectura, versión del protocolo y la dirección donde se instaló.

[43] PPA, *Personal Package Archives*, es el repositorio de confianza que contiene las versiones últimas y estables para instalar de forma sencilla *go-ethereum, geth,* en la distribución de Ubuntu.

```
alexita@SisAlarmasMinero: ~
alexita@SisAlarmasMinero:~$ sudo apt-get install geth
Reading package lists... Done
Building dependency tree
Reading state information... Done
geth is already the newest version (1.8.6+build13246+xenial).
0 upgraded, 0 newly installed, 0 to remove and 121 not upgraded.
alexita@SisAlarmasMinero:~$ geth version
Geth
Version: 1.8.6-stable
Git Commit: 12683feca7483f0b0bf425c3c520e2724f69f2aa
Architecture: 386
Protocol Versions: [63 62]
Network Id: 1
Go Version: go1.10
Operating System: linux
GOPATH=
GOROOT=/usr/lib/go-1.10
```

Figura 2.19 Instalación y comprobación de Geth

- Después de instalar el *geth*, se procede a implementar la red privada de *blockchain* usando el mismo bloque génesis en los dos mineros, donde se va a crear el *ledger* inicial en cada minero.

  La figura 2.20 detalla la creación de la *blockchain* del primer minero, además se indexa exitosamente el bloque génesis al minero, todo este proceso se realiza en la carpeta principal, ChainSkills. Este mismo proceso se repite para el segundo minero.

```
alexita@SisAlarmasMinero: ~/ChainSkills
alexita@SisAlarmasMinero:~$ cd ~/ChainSkills
alexita@SisAlarmasMinero:~/ChainSkills$ geth --datadir ~/ChainSkills/minero1
 init genesis.json
INFO [04-30|15:33:24] Maximum peer count                       ETH=25 LES=0
total=25
INFO [04-30|15:33:24] Allocated cache and file handles         database=/hom
e/alexita/ChainSkills/minero1/geth/chaindata cache=16 handles=16
INFO [04-30|15:33:24] Writing custom genesis block
INFO [04-30|15:33:24] Persisted trie from memory database      nodes=0 size=
0.00B time=6.191µs gcnodes=0 gcsize=0.00B gctime=0s livenodes=1 livesize=0.0
0B
INFO [04-30|15:33:24] Successfully wrote genesis state         database=chai
ndata                                          hash=274f18…fa200b
INFO [04-30|15:33:24] Allocated cache and file handles         database=/hom
e/alexita/ChainSkills/minero1/geth/lightchaindata cache=16 handles=16
INFO [04-30|15:33:24] Writing custom genesis block
INFO [04-30|15:33:24] Persisted trie from memory database      nodes=0 size=
0.00B time=4.071µs gcnodes=0 gcsize=0.00B gctime=0s livenodes=1 livesize=0.0
0B
INFO [04-30|15:33:24] Successfully wrote genesis state         database=ligh
tchaindata                                          hash=274f18…fa200b
```

Figura 2.2 Implementación del bloque genesis en el minero

- La figura 2.21 muestra que después de crear los mineros, automáticamente se generan dos subcarpetas: *geth* y *keystore*[44]. En la carpeta *geth* se crea unos archivos que contienen el libro de transacción, *ledger* o base de datos de la cadena de bloques privada.

```
alexita@SisAlarmasMinero: ~
alexita@SisAlarmasMinero:~$ ls ~/ChainSkills/minero1
geth  keystore
alexita@SisAlarmasMinero:~$ ls ~/ChainSkills/minero2
geth  keystore
alexita@SisAlarmasMinero:~$ ls ~/ChainSkills/minero1/geth
chaindata  lightchaindata
alexita@SisAlarmasMinero:~$ ls ~/ChainSkills/minero2/geth
chaindata  lightchaindata
```

Figura 2.21 Generación de los archivos geth y keystore en los mineros

- Ahora, en la figura 2.22 se crea manualmente las cuentas, *accounts*, para cada minero. La primera *account* es una cuenta por default, que se crea para correr el nodo. Proceso similar se realiza en el otro minero para crear sus correspondientes cuentas, con el comando *account new*. Cabe recalcar que cada cuenta tiene su propia dirección y contraseña robusta.

```
alexita@SisAlarmasMinero: ~
alexita@SisAlarmasMinero:~$ geth --datadir ~/ChainSkills/minero1 account new
INFO [04-30|17:08:42] Maximum peer count                       ETH=25 LES=0
total=25
Your new account is locked with a password. Please give a password. Do not f
orget this password.
Passphrase:
Repeat passphrase:
Address: {7f9bf0b5c21945217acded26bc951cc4e9f3cb3f}
alexita@SisAlarmasMinero:~$ geth --datadir ~/ChainSkills/minero1 account new
INFO [04-30|17:16:26] Maximum peer count                       ETH=25 LES=0
total=25
Your new account is locked with a password. Please give a password. Do not f
orget this password.
Passphrase:
Repeat passphrase:
Address: {e8a469d2d6a9b8820fdc5935bb69049c33249a15}
```

Figura 2.22 Creación de las cuentas en el minero

- La figura 2.23 indica la comprobación de las cuentas en cada minero por medio del comando *account list*.

[44] *keystore* se localizará el monedero, *wallet*, para almacenar las cuentas que va a manejar el nodo.

```
alexita@SisAlarmasMinero: ~
alexita@SisAlarmasMinero:~$ geth --datadir ~/ChainSkills/minero1 account list
INFO [05-01|18:04:27] Maximum peer count                       ETH=25 LES=0 tota
l=25
Account #0: {7f9bf0b5c21945217acded26bc951cc4e9f3cb3f} keystore:///home/alexita/
ChainSkills/minero1/keystore/UTC--2018-05-01T00-09-10.095094377Z--7f9bf0b5c21945
217acded26bc951cc4e9f3cb3f
Account #1: {e8a469d2d6a9b8820fdc5935bb69049c33249a15} keystore:///home/alexita/
ChainSkills/minero1/keystore/UTC--2018-05-01T00-16-51.996949316Z--e8a469d2d6a9b8
820fdc5935bb69049c33249a15
alexita@SisAlarmasMinero:~$ geth --datadir ~/ChainSkills/minero2 account list
INFO [05-01|18:04:44] Maximum peer count                       ETH=25 LES=0 tota
l=25
Account #0: {fc6e28647435538e800f8504fe823d788b1cc08f} keystore:///home/alexita/
ChainSkills/minero2/keystore/UTC--2018-05-01T18-38-17.710163615Z--fc6e2864743553
8e800f8504fe823d788b1cc08f
Account #1: {d0c508fd9525192058fdd032bfd1845e1df50786} keystore:///home/alexita/
ChainSkills/minero2/keystore/UTC--2018-05-01T18-39-41.628819143Z--d0c508fd952519
2058fdd032bfd1845e1df50786
```

Figura 2.23 Listado de cuentas asignadas a cada minero

- Otra forma de comprobar las cuentas que pertenecen a cada minero es mediante el *keystore* como indica la figura 2.24 e indica donde se almacena la *wallet*, los permisos que posee y su correspondiente dirección.

```
alexita@SisAlarmasMinero: ~
alexita@SisAlarmasMinero:~$ ls -al ~/ChainSkills/minero1/keystore
total 16
drwx------ 2 alexita alexita 4096 Apr 30 17:17 .
drwxrwxr-x 4 alexita alexita 4096 May  1 18:07 ..
-rw------- 1 alexita alexita  491 Apr 30 17:10 UTC--2018-05-01T00-09-10.09509437
7Z--7f9bf0b5c21945217acded26bc951cc4e9f3cb3f
-rw------- 1 alexita alexita  491 Apr 30 17:17 UTC--2018-05-01T00-16-51.99694931
6Z--e8a469d2d6a9b8820fdc5935bb69049c33249a15
alexita@SisAlarmasMinero:~$ ls -al ~/ChainSkills/minero2/keystore
total 16
drwx------ 2 alexita alexita 4096 May  1 11:39 .
drwxrwxr-x 4 alexita alexita 4096 May  1 16:05 ..
-rw------- 1 alexita alexita  491 May  1 11:38 UTC--2018-05-01T18-38-17.71016361
5Z--fc6e28647435538e800f8504fe823d788b1cc08f
-rw------- 1 alexita alexita  491 May  1 11:39 UTC--2018-05-01T18-39-41.62881914
3Z--d0c508fd9525192058fdd032bfd1845e1df50786
```

Figura 2.24 *Wallet* de los mineros

- La figura 2.25 indica el archivo en texto plano, *password*.sec, que contiene la contraseña de la primera cuenta que se creó en el minero, dentro de su directorio principal.

```
alexita@SisAlarmasMinero: ~/ChainSkills/minero1
alexita@SisAlarmasMinero:~$ cd ~/ChainSkills/minero1
alexita@SisAlarmasMinero:~/ChainSkills/minero1$ gedit password.sec
alexita@SisAlarmasMinero:~/ChainSkills/minero1$ geth --identity "minero1" --netw
orkid 42 --datadir "~/ChainSkills/minero1" --nodiscover --mine --rpc --rpcport "
8042" --port "30303" --unlock 0 --password ~/ChainSkills/minero1/password.sec --
ipcpath "~/Library/Ethereum/geth.ipc"
INFO [04-30|17:45:13] Maximum peer count                       ETH=25 LES=0 tota
l=25
INFO [04-30|17:45:13] Starting peer-to-peer node               instance=Geth/min
ero1/v1.8.6-stable-12683fec/linux-386/go1.10
INFO [04-30|17:45:13] Allocated cache and file handles         database=/home/al
exita/ChainSkills/minero1/geth/chaindata cache=768 handles=512
```

Figura 2.25 Iniciando el minero por medio de Geth

Lo siguiente es iniciar el minero con el comando geth, considerando los siguientes parámetros [57]:

- *Identit*y: nombre del minero que se referencia en la red privada.
- *networkid*: valor que identifica a la red igual al valor del bloque génesis.
- *datadir*: carpeta donde se almacena el minero de la *blockchain* privada.
- *nodiscover:* mecanismo para el descubrimiento del resto de nodos. Como sólo se está probando este minero esta desactivada esta función.
- *mine:* permite minar los ethers y las transacciones
- *rpc* y *rpcport:* permite habilitar el servidor HTTP, RPC a través del número de puerto.
- *port:* número de puerto donde los nodos están conectados entre sí y se propagan las nuevas transacciones o bloques.
- *unlock:* identificar de la cuenta por *default*.
- *password:* indica la ubicación donde se encuentra la contraseña de la cuenta por *default*.
- *ipcpath*: ruta del socket IPC, permite iniciar la *blockchain* privada con el navegador de Mist, mediante el archivo geth.ipc sin necesidad de ejecutar el Geth.

- De esta manera en la figura 2.26 se realiza el *script* ejecutable, *startminero1*, del comando Geth con similares parámetros que el *password.sec*. Posteriormente se procede a cambiar los permisos de ejecución del script y luego proceder a ejecutar este. Como resultado de este proceso, el minado comienza y la cuenta por *default* recibe ethers minados por el nodo. Este proceso se puede ver directamente con el navegador de Mist, pero esos ethers sólo sirven para esta *blockchain* privada.

```
alexita@SisAlarmasMinero: ~/ChainSkills/minero1
alexita@SisAlarmasMinero:~/ChainSkills/minero1$ gedit startminero1.sh
alexita@SisAlarmasMinero:~/ChainSkills/minero1$ ls
geth  keystore  password.sec  startminero1.sh
alexita@SisAlarmasMinero:~/ChainSkills/minero1$ chmod +x startminero1.sh
alexita@SisAlarmasMinero:~/ChainSkills/minero1$ ls
geth  keystore  password.sec  startminero1.sh
alexita@SisAlarmasMinero:~/ChainSkills/minero1$ ./startminero1.sh
INFO [04-30|19:29:18] Maximum peer count                       ETH=25 LES=0 tota
l=25
INFO [04-30|19:29:19] Starting peer-to-peer node               instance=Geth/min
ero1/v1.8.6-stable-12683fec/linux-386/go1.10
INFO [04-30|19:29:19] Allocated cache and file handles         database=/home/al
exita/ChainSkills/minero1/geth/chaindata cache=768 handles=512
INFO [04-30|19:29:21] Initialised chain configuration          config="{ChainID:
 42 Homestead: 0 DAO: <nil> DAOSupport: false EIP150: <nil> EIP155: 0 EIP158: 0
Byzantium: <nil> Constantinople: <nil> Engine: unknown}"
INFO [04-30|19:29:21] Disk storage enabled for ethash caches   dir=/home/alexita
/ChainSkills/minero1/geth/ethash count=3
```

Figura 2.26 Creación y ejecución del *script*

Para crear el segundo minero se siguen los mismos pasos anteriores, es decir, crear este minero en el mismo directorio raíz e iniciar el mismo bloque génesis. Además, se crea el *default account*, *wallet* y el archivo password.sec. La figura 2.27 indica la variación del segundo minero, se presenta en los atributos de los parámetros del nuevo *script* ejecutable. Presenta el mismo identificador de red, pero diferentes atributos en el nombre del minero, puerto (se implementa la simulación en el mismo computador) y no incluye con el parámetro *ipcpath*. Por consiguiente, el archivo geth.ipc es creado manualmente por consola en el directorio del minero. Al mirar este archivo existen nuevos atributos como: admin, debug, eth, miner, net, personal, rpc, shh, txpool y web3, que van a permitir minar la cadena de bloques.

```
startminero2.sh (~/ChainSkills/minero2) - gedit                    9:07 PM
Open ▾                                                              Save
#!/bin/bash

geth --identity "minero2" --dev --networkid 42 --datadir "~/ChainSkills/minero2"
--nodiscover --mine --rpc --rpcport "8643" --rpcapi "db,eth,net,web3,miner" --
port "30304" --unlock 0 --password ~/ChainSkills/minero2/password.sec
```

Figura 2.27 Script con los parámetros del segundo minero.

Todos estos pasos se repiten para añadir más nodos a la red privada de *Ethereum*, considerando los siguientes criterios:

- Trabajar con el mismo archivo génesis y el mismo identificador de red.
- Cambiar el puerto si se usa el mismo RPi para crear varios nodos.
- Añadir en el archivo static-nodes.json manualmente la información de cada nodo (clave encriptada, dirección IP y puerto).

Existen diferentes formas para administrar el minero o nodo.

1. Usando *Geth Javascript console*, se puede minar o enviar transacciones a través de la consola de Javascript Geth, por el comando geth attach. Esta instrucción no necesita de un parámetro adicional por la ayuda del archivo geth.ipc que está dentro del directorio principal.

2. Para iniciar o parar la ejecución del minero o archivo se usa *start y stop* respectivamente.

Existen algunas opciones para terminar el proceso de minado, por ejemplo:

1. Presionando las teclas CTRL+C en la consola.

2. Matar el proceso, pero antes es necesario buscar el identificador del proceso que está corriendo y colocar ese valor en el comando *kill.*

Para borrar los datos del minero en la cadena de bloques:

1. Usar el comando rm –rf y especificar el directorio donde se va a borrar el minero.

Desarrollo del contrato inteligente

El contrato inteligente tendrá un conjunto de direcciones que están asociadas a un número de *tokens*. Estos *tokens* identifican al usuario con su respectiva dirección que va a estar relacionada con un servicio específico. Si el *token* es mayor a 0 implementa un servicio, si es igual a 0 no requiere el servicio.

- Se instala *truffle* que va a permitir desarrollar el contrato inteligente en *Ethereum*, con la ayuda del comando *install*. El contrato se crea en el mismo directorio donde se encuentra el minero y el nodo. Luego se procede a iniciar el proyecto mediante el comando *truffle init.*

- Después, se procede a crear un archivo con el nombre del token. En este caso se usa el identificativo de AlarmToken.sol y hace referencia al token que se va a transferir en el sistema de alarmas a través de la cadena de bloques.

- Luego se especifica algunas propiedades, por ejemplo, el nombre de la red y el número de puerto. Se corre el comando *truffle migrate* para compilar el contrato. Otra opción para crear el contrato inteligente es por medio la página oficial de *Ethereum* https://www.ethereum.org/.

- La ventaja de trabajar con la página oficial es el manejo directo con el estándar ERC20, donde solo es necesario descargar el archivo para crear un *token* digital de la red privada de *Blockchain*. Específicamente, en el sistema de alarmas residenciales el *token* va a llevar los eventos de emergencia y puede ser compatible en otra aplicación descentralizada que trabaje bajo el estándar ERC20.

- Para compilar el contrato inteligente se puede usar la consola Geth o el navegador de Mist. Si se considera implementar el contrato en el navegador de *Mist*, es necesario descargar la última versión de la página oficial: https://github.com/ethereum/mist/releases/

- Finalmente, se procede a crear el contrato AlarmToken con su respectiva dirección y completando los parámetros del ABI[45]. En el contrato inteligente dentro de ese archivo indica que la señal de los eventos procede del panel de control a través de sus salidas programables.

Recepción de los eventos de alarma desde el panel hacia el Raspberry Pi 3

El RPI se utiliza como nodo en la cadena de bloques de la red P2P. Uno de los pines del GPIO que manejan un bucle de lectura será conectado a la salida de sirena del panel, adicional se puede leer un par de pines conectados a una o varias salidas programables del panel configuradas para monitorear algún tipo de condición específica para la gestión de los eventos. Finalmente se puede utilizar un pin más de entrada del Raspberry Pi para un pulsante del botón de pánico.

La figura 2.28, muestra un ejemplo de código abierto mediante Python para controlar los pines GPIO del RPI mediante la librería gpiozero[46].

```
from gpiozero import Button
from time import sleep

button = Button(2)

while True:
    if button.is_pressed:
        print("Pressed")
    else:
        print("Released")
    sleep(1)
```

Figura 2.28 Ejemplo de la configuración de GPIO del RPI [58]

[45] ABI, *Application Binary Interface*, es la aplicación de la interfaz de la consola de truffle.
[46] La librería gpiozero incluye una interfaz sencilla para manejar en el Raspberry Pi los GPIO [63].

Las salidas programables, PGM, del panel de alarma se configuran mediante cambios en los registros internos del equipo. Por ejemplo, la figura 2.29 muestra la programación de los eventos que se pueden realizar en el panel DSC 1832, donde la salida programable se encuentra en los registros número 009 – 010.

[009-010] Programación PGM
PGMs 3&4 se aplican solamente al PC1864

[009]	Programación de Salida PGM de la Tarjeta Principal		
Def		Insiera 2 dígitos [01]-[32]	
19	I___II___I	PGM 1	Sección [009]
10	I___II___I	PGM 2	Sección [009]
01	I___II___I	PGM 3	Sección [010] ... PC1864 Solamente
			Sección [010] ... PC1864 Solamente
01	I___II___I	PGM 4	

01 Salida de Incendio y Robo	17 Status de Armado Away
02 No utilizado	18 Status de Armado Stay
03 Restauración de Sensor(✱72)	19 Salida de Mando #1 (✱71)
04 Detector de Humo de 2 Hilos (PGM2)	20 Salida de Mando #1 (✱72)
05 Status Armado	21 Salida de Mando #1 (✱73)
06 Listo para Armar	22 Salida de Mando #1 (✱74)
07 Modo de seguimiento de la sirena del teclado	23 Entrada Silenciosa 24 h
08 Pulso de Advertencia	24 Alarma Audible 24 h
09 Salida de Problema del Sistema (con Opciones de Problema)	25 Salida de Incendio y Robo Retardada
10 Evento del Sistema (con Opciones de Evento)	26 Salida de Prueba de Batería
11 Antiviolación del Sistema (Todas las Fuentes)	27 Salida del Código de Policía
12 TLM y Alarma	28 Salida de Coacción
13 Salida de Desconexión	29 Salida Invertida de Seguimiento de Zona
14 Pulso de Iniciación de Conexión a Tierra	30 Salida de Memoria de la Alarma de Status de la Partición
15 Operación Remota	31 Comunicaciones Alternas
16 Uso Futuro	32 Abrir Después de Alarma (Cancelar Código)

Figura 2.29 Salidas PGMs en el panel DSC 1832

Al momento de conectar una salida PGM, en un panel DSC1832 al RPI, se debe proteger el circuito de algún cambio de voltaje o corriente, es decir, aislar a los dispositivos eléctricamente por medio de un circuito adicional. El manual del panel DSC1832 recomienda usar una salida de relé como se muestra en la figura 2.30.

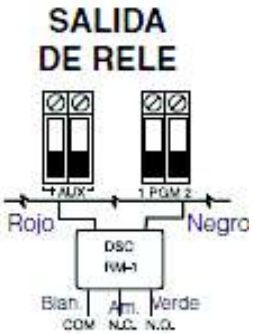

Figura 2.30 Conexión del relé a la salida PGM del panel DSC1832 [5]

Una vez captado el cambio de estado en el pin de entrada destinado al monitoreo, la información deberá ser incluida por el nodo a la cadena de bloques por medio de una transacción o contrato inteligente.

La configuración más sencilla del PC1832, considerando las 6 zonas en base a la distribución de puntos de la casa tipo, con el teclado LCD 5511. Con contraseña del administrador, 5555 y el respectivo registro de zonas, se considera las primeras tres zonas para el contacto magnético, la zona 4 para los sensores de movimiento y la zona 5 para el detector de humo. El botón de pánico y la sirena se conectarán directamente al RPI.

Los atributos de las salidas programables se manejan con la opción 501 para la primera PGM y 502 para PGM2. En la zona del detector de movimiento, se considera un tiempo de retardo para que el usuario pueda ingresar o salir de su hogar antes que digite su clave y suene la sirena; estos registros se programan con opción 005 en minutos.

La figura 2.31 indica un evento de intrusión en la zona 1, el led verde indica que esa señal ingresa a la PGM1, el led rojo indica que se activa la sirena, para simular la sirena se usa una luz piloto a través de un relé que se conecta a la entrada del GPIO del RPI.

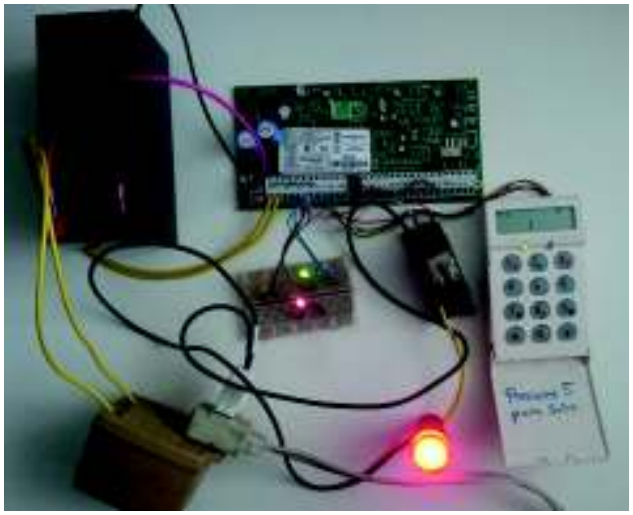

Figura 2.31 Esquema de una intrusión en una zona en el panel

Notificación de los eventos a los usuarios de la red

El sistema descentralizado permite a todos los usuarios de la red, conocer el registro distribuido público, *ledger,* de todas las transacciones, eventos, en la cadena de bloques. Estos eventos de alarma, se reportarán directamente a los miembros de la red privada, 30 usuarios de la red y al UPC, para que puedan participar en el consenso de la información y en la seguridad comunitaria.

La información puede ser exteriorizada mediante una interfaz de usuario o de forma sonora, de tal forma que las personas participantes conozcan el estado de la alarma y puedan dar asistencia de ser el caso. La sirena, seguirá trabajando de manera similar que en el sistema de alarmas centralizado. Se activa emitiendo un ruido, para indicar que existe un evento de emergencia.

El usuario puede recibir notificaciones de los eventos a través de su dispositivo móvil, se puede programar en una *app* las salidas de alarma con un hilo, para tomar la información del evento y canalizar esta mediante un socket que reporta localmente hacia los celulares de los usuarios que estén presentes en sus hogares.

Una aplicación web, permite que remotamente los usuarios visualicen y auditen el registro de las transacciones de los eventos a cualquier hora. Esta interfaz web permite a los usuarios en caso de emergencia, aplicar los protocolos de seguridad planificados por la comunidad y además proporciona una comunicación directa con el personal de la UPC.

Se puede conectar un dispositivo adicional a la línea telefónica, para emitir notificaciones de voz o mensaje a números preasignados por los usuarios ante la presencia de una intrusión, así como, Dialer. También se puede trabajar con las salidas programables (PGM) del panel incorporando módulos extras, por ejemplo, *GPRS* para cuando se cierra un contacto se manda un mensaje.

Por Internet, a través del TL-150 que se conectan a cualquier panel DSC o puede conectarse directamente a la red *P2P*, apuntando a la dirección *IP* de los mineros. Mediante el Raspberry Pi, conectando a un pin un dispositivo para para realizar llamadas automáticas e enviar mensajes del historial del evento. Se puede desarrollar una aplicación descentralizada, para notificar los eventos al usuario por medio del *IoT*.

2.3. Fase de análisis de costos

Presupuesto del sistema de alarmas tradicional

El presupuesto de instalación del sistema de alarmas convencionales fue elaborado utilizando análisis de precios unitarios, además se encuentra detallado en función del análisis de costos de los equipos, monitoreo, la instalación y mantenimiento.

El análisis de precios unitarios (APU), es una técnica muy utilizada en las empresas para elaborar presupuestos, tiene un desglose en los rubros que componen una obra. Comúnmente el APU es una técnica muy utilizado por los diseñadores de ingeniería y arquitectura para obras de construcción; son expresados en forma de unidad, no globalmente.

El valor total de cada rubro es la suma de los costos directos e indirectos. Los costos directos de cada uno de los rubros se dividen en las siguientes secciones: herramienta, mano de obra, materiales y transporte. En cambio, los costos indirectos son un porcentaje de los costos directos y se compone de gastos administrativos y financieros, en este porcentaje se incluye la ganancia.

En la elaboración del presupuesto se considera el valor de herramienta al 5% de la mano de obra para simplificar el cálculo. Además, se considera $0 el valor del transporte por cada casa, puesto que no se necesitan camionetas o cualquier otro vehículo adicional. El presupuesto no incluye impuesto al valor agregado vigente.

Análisis de costo de Equipos

Para el análisis del coste de los equipos se considera la cotización presente en el Anexo VI que muestra el precio de provisión local de acuerdo a la oferta del mercado.

La tabla 2.5 desglosa el cálculo del costo del equipamiento. En el Anexo VII, se detalla el coste por partes de acuerdo al sensor de movimiento, detector de humo, botón de pánico, contacto magnético, teclado de control, panel de alarmas y sirena exterior. La cantidad de puntos se tomó como referencia de los planos arquitectónicos.

Tabla 2.5 Cálculo del costo de equipos

Cod.	Descripción	Unidad	Cant.	P. Unitario ($)	Total ($)
1	Sensor de movimiento	U	5,00	12,56	62,80
2	Detector de humo	U	1,00	17,28	17,28
3	Botón de pánico	U	4,00	24,92	99,68
4	Contacto magnético	U	4,00	2,47	9,88
5	Teclado de control	U	1,00	63,58	63,58
6	Panel de alarmas incluye teclado y caja	U	1,00	153,12	153,12
7	Sirena exterior	U	1,00	32,20	32,20
			TOTAL:		**$438,54**

Análisis del costo de monitoreo

La tabla 2.6 indica el coste del monitoreo en base al promedio de dos cotizaciones que se solicitó a dos empresas de monitoreo, LAARCOM y CGB. La descripción de servicios y costos se detalla en el Anexo VIII. El cliente registra un pago mensual por el monitoreo del servicio del sistema de alarmas. El **costo anual** del servicio de monitoreo sería de **$330.00**.

Tabla 2.6 Cálculo del costo de Monitoreo

Cod.	Descripción	Horas	Cant.	P. Unitario ($)	Total ($)
1	Monitoreo del sistema de alarmas CGB	24	1,00	29,50	29,50
2	Monitoreo del sistema de alarmas LAARCOM	24	1,00	26,00	25,50
			TOTAL PROMEDIO:		**$27,50**

LAARCOM

Ofrece respuesta armada con un máximo de 10 minutos de respuesta solicitando también apoyo policial, estos tiempos dicen poder cumplirlos debido a sus bases móviles. Ofrecen servicio de notificación por correo electrónico cuando el sistema es armado o desarmado. El costo de este servicio a febrero del 2018 es de $25.50, este precio no incluye IVA.

CGB

Dispone de algunos servicios distintos dependiendo de la tarifa. El monitoreo que se va centrar en este estudio tiene un costo de $29.50 + IVA ofreciendo un monitoreo 24/7, una

conexión directa con la UPC más cercana, la verificación física motorizada. Esta empresa no pudo precisar el tiempo de respuesta específico pues depende de la ubicación del sitio a monitorear. El personal asignado por la empresa partiría con su motocicleta desde la oficina más cercana (sector El Labrador, Puembo o El Condado) hasta la residencia.

Análisis del costo de instalación y mantenimiento

Al momento de realizar el análisis de costo de instalación del sistema de alarmas es adecuado diferenciar el costo del equipamiento (costo de equipo) del costo de los puntos (costo de instalación necesaria para la conexión del equipo en sí). En el mejor de los casos la instalación de los puntos se considera en obra durante la construcción de la casa. Este valor presupuestado se encuentra en la tabla 2.7 e indica los puntos necesarios para alarma tipo A y B, panel de alarmas, teclado y sirena, que se toman como base del plano arquitectónico de la casa tipo.

El presente estudio considera para la instalación del sistema de alarmas una cuadrilla de técnicos electricistas conformada por un maestro electricista y un ayudante. Adicional para realizar las conexiones de panel y configuraciones se requiere de un ingeniero electrónico. Las horas de trabajo del personal, materiales y herramienta se muestran en el presupuesto con análisis de precios unitario detallado en el Anexo IX. Este valor incluye la tubería, accesorios y cableado interior.

Por otro lado, este es el valor adicional de una casa nueva con los servicios embebidos y con tubería EMT. El costo puede disminuir sustancialmente con el uso de manguera negra eléctrica durante la ejecución en obra.

Tabla 2.7 Cálculo del costo de instalación

Cod.	Descripción	Unidad	Cant.	P. Unitario ($)	Total ($)
1	Punto para alarma tipo A	Punto	6,00	21,24	127,44
2	Punto para alarma tipo B	Punto	8,00	19,48	155,84
3	Punto para panel de alarmas	Punto	1,00	47,53	47,53
4	Punto para teclado	Punto	2,00	19,48	38,96
5	Punto para sirena	Punto	1,00	17,46	17,46
			TOTAL:		**$387,23**

Lo más común en el mercado de la construcción es no considerar estos servicios durante la construcción de la casa, en tal caso se suele usar silicona para la fijación de cables y su paso por cortineras, barrederas, detalles de cielo falso, etc.; esto disminuye el valor de instalación aún más, a pesar de no ser una práctica recomendable es bastante común que las empresas de monitoreo recurran a esto para disminuir los costos del servicio para sus clientes.

Con respecto al costo de mantenimiento, los paneles de alarma convencionales emiten eventos de mantenimiento los cuales tienen que ser atendidos por la empresa contratada para el monitoreo. Por lo general, la empresa realiza visitas técnicas y un mantenimiento periódico sin costo adicional al valor mensual por el servicio de monitoreo.

La tabla 2.8 despliega el costo total necesario de equipamiento, monitoreo, instalación y mantenimiento del sistema de alarmas centralizado convencional, el cual suma un valor de $1.155,77 por cada casa. Por lo tanto, el Anexo X detalla el desglose mensual y anual de las 30 casas; cuyo valor mensual ascendería a **$34.673.10 Treinta y cuatro mil seis cientos setenta y tres dólares con diez centavos**, sin incluir el IVA.

Tabla 2.8 Cálculo del presupuesto mensual del Sistema de Alarmas Centralizado

Cod.	Tipo de costo	Total
1	Equipamiento	**$**438,54
2	Monitoreo	**$**330,00
3	Instalación	**$**387,23
4	Mantenimiento	**$**0,00
	TOTAL	***$1.155,77**

MIL CIENTO CINCUENTA Y CINCO dólares SETENTA Y SIETE centavos.

NOTA: * Este presupuesto no incluye el IVA vigente

Presupuesto del nuevo sistema de alarmas con la Tecnología *Blockchain*

El sistema de alarmas considerando la nueva tecnología *Blockchain* parte del costo de instalación del sistema de alarmas convencionales; involucra el mismo número de puntos y sensores en la tecnología *Blockchain*. Adicionalmente, comprende un coste con respecto a los materiales, gastos de instalación de los nodos y mineros, operación y mantenimiento.

Análisis de costo de materiales o accesorios

En el análisis de los gastos de los materiales, se van a considerar dos escenarios, dependiendo de la situación de las 30 casas en estudio.

Opción A, que al menos en cualquiera de las 30 casas, existan 4 computadores personales (ver los requerimientos de hardware mínimo en la tabla 2.9) adecuados para levantar los mineros dentro de la red *Ethereum* privada, entonces sólo se considera el gasto de los accesorios del *Raspberry Pi* para implementar los nodos en cada casa. Estos valores se toman en base de la cotización que se encuentra en el Anexo XI.

Tabla 2.9 Cálculo del hardware para el sistema de alarmas con Tecnología *Blockchain*. Opción A

Cod.	Descripción	Unidad	Cant.	P. Unitario ($)	Total ($)
1	Fuente de Raspberry	U	1.00	11.16	11.16
2	Raspberry Pi 3	U	1.00	58.04	58.04
3	Disipador de calor para RPI	U	1.00	10.71	10.71
4	Ventilador 1.5" 12V 0.1A	U	1.00	4.46	4.46
5	MicroSD 16GB	U	1.00	16.00	16.00
			TOTAL:		**$100.37**

Opción B, no existan algún computador personal en alguna de las 30 casas que cumple con las características mínimas necesarias para implementar los mineros. La tabla 2.10 detalla el cálculo del hardware adicional para el sistema de alarmas, considerando la cotización que se detalla en Anexo XII. Todos los materiales y accesorios son estándares y fáciles de conseguir en el mercado local.

Tabla 2.10 Cálculo del hardware para el sistema de alarmas con Tecnología *Blockchain.* Opción B

Cod.	Descripción	Unidad	Cant.	P. Unitario ($)	Total ($)
1	Fuente de Raspberry	U	1.00	11.16	11.16
2	Raspberry Pi 3	U	1.00	58.04	58.04
3	Disipador de calor para RPI	U	1.00	10.71	10.71
4	Ventilador 1.5" 12V 0.1A	U	1.00	4.46	4.46
5	MicroSD 16GB	U	1.00	16.00	16.00
6	CPU Q-One core i3-7100 4GB 1Tb	U	1.00	470.39	470.39
			TOTAL:		**$570.76**

Análisis de costo de Instalación

La tabla 2.11 muestra el cálculo del costo de instalación del software que se necesita para empezar a configurar el minero en la PC, mediante la distribución de Ubuntu versión 16.04, y el nodo con Rasbian en el *Raspberry Pi* 3; tal como se indica en el Anexo XIII. Para la instalación de la red *Ethereum* privada se cuenta con la asistencia de un Ingeniero y un técnico. Al trabajar con software libre no es necesario un costo adicional de licencias por instalar el sistema operativo en la red.

Tabla 2.11 Cálculo del costo de instalación del software para red P2P

Cod.	Descripción	Cant.	Precio/hora ($)	Total ($)
1	Instalación del nodo en el Raspberry	30.00	3.30	99.00
2	Instalación del minero en la PC	4.00	12.73	50.92
		TOTAL:		**$149.92**

Análisis de costo de Operación

El costo de operación de la tecnología *Blockchain*, por su característica de servicio autónomo e independiente, serian despreciables, ya que no se necesita de ningún técnico que verificando la gestión de los eventos o realice el monitoreo las 24 horas del día, los 365 días del año. El sistema de alarma va a funcionar con la colaboración de todas las partes dentro de la red.

Análisis de costo de Implementación de nodos y mineros

Los gastos de implementación se refieren a los costos que implica el funcionamiento de nodos y mineros en la red P2P *Ethereum* privada como se muestra en la tabla 2.12.

Tabla 2.12 Cálculo del costo de operación de la red P2P *Ethereum* Privada

Cod.	Descripción	Cant.	Precio/hora ($)	Total ($)
1	Nodo en el RPI	30.00	30.23	906.90
2	Minero en la PC	4.00	24.73	98.92
3	Ejecución del contrato inteligente	1.00	27.48	27.48
		TOTAL:		**$1,033.30**

En esta parte se consideran los elementos básicos de la tecnología Blockchain que involucra a nodos, mineros y contrato inteligente. El detalle de los valores se encuentra en el Anexo XIV, asumiendo un costo estimado de volumen por hora de un Ingeniero en Sistemas en función de las demandas del mercado local.

Análisis de costo de Mantenimiento

La implementación y funcionamiento del sistema de alarmas descentralizado con la plataforma de *Ethereum* requiere cierto mantenimiento periódico para garantizar un buen servicio y detectar cualquier daño o reemplazo en algún equipo por ejemplo en el RPI o mal funcionamiento en la red *P2P*; lo que puede afectar la gestión de los eventos de alarma o emergencia. La tabla 2.13 muestra el cálculo del costo de mantenimiento de los 30 nodos y 4 mineros, tanto en las casas como en la oficina del UPC más cercano a estas, cuyo tiempo máximo de asistencia es de 3 horas.

Tabla 2.13 Cálculo del costo de mantenimiento de la red P2P *Ethereum* Privada

Cod.	Descripción	Costo mensual ($)	N° pagos	Total ($)
1	Mantenimiento de red P2P	13.46	4.00	53.84
		TOTAL ANUAL		**$53.84**

La tabla 2.14 especifica el presupuesto total para el sistema de alarmas con la Tecnología *Blockchain* utilizando la plataforma *Ethereum* privada.

Tabla 2.14 Cálculo del presupuesto total del Sistema de Alarmas en base a la Tecnología *Blockchain*. Opción A.

Cod.	Tipo de costo	Total ($)
1	Equipamiento del sistema de alarmas	13,156.20
2	Instalación del sistema de alarmas	11,616.90
3	Materiales adicionales para red descentralizada	3,011.10
4	Instalación red *Ethereum* Privada	149.92
5	Operación del sistema de alarmas	0.00
6	Implementación de la red P2P	1,033.30
7	Mantenimiento de la red P2P	53.84
	TOTAL	***$29,021.26**

VEINTE Y NUEVE MIL VEINTE Y UNO dólares y VEINTE Y SEIS centavos

*NOTA: no incluye IVA vigente

Considerando el escenario A de los materiales adicionales con la Plataforma Ethereum Privada, a este presupuesto de suma el costo del equipo y de la instalación del sistema de alarmas convencionales de las 30 casas. Todos los costos de instalación, operación y mantenimiento de la red P2P se presentan para todas las 30 casas y con respecto a un costo anual de estos servicios.

En la tabla 2.15 indica la opción B, donde se considera que no existe ningún computador personal para implementar el minero. Para obtener el costo del presupuesto total se sigue las mismas consideraciones que en la tabla 2.16, es decir, se suma el costo de equipos e instalación de los puntos y sensores del sistema de alarmas y se le añade el coste del nuevo hardware, considerando el costo de los 4 CPUs adicionales a los 30 RPI y demás accesorios, el costo de instalación, operación y mantenimiento de la red P2P. Todos estos valores se calculan anualmente y para las 30 casas.

Tabla 2.15 Cálculo del presupuesto total del Sistema de Alarmas en base a la Tecnología *Blockchain*. Opción B.

Cod.	Tipo de costo	Total ($)
1	Equipamiento del sistema de alarmas	13,156.20
2	Instalación del sistema de alarmas	11,616.90
3	Materiales adicionales	4,892.66
4	Instalación red *Ethereum* Privada	149.92
5	Operación del sistema de alarmas	0.00
6	Implementación de la red P2P	1,033.30
7	Mantenimiento de la red P2P	53.84
	Total	***$30,902.82**

Treinta mil novecientos dos dólares ochenta y dos centavos

*Nota: no incluye IVA vigente

3. RESULTADOS Y DISCUSIÓN

En esta parte se va a presentar los resultados más relevantes obtenidos del análisis de la plataforma *Ethereum*, la comparación de los sistemas de alarmas convencionales y el nuevo sistema de alarmas con la Tecnología *Blockchain* para la gestión de la información de los eventos y su respectivo análisis de costos

3.1. Análisis de la plataforma *Ethereum*

Análisis del precio de una transacción

La mayoría de plataformas distribuidas manejan el algoritmo de consenso en base a la *PoW*. Para procesar las transacciones o contratos inteligentes conlleva un costo, *Gas*, que está en manos del usuario, quien decide cuánto está dispuesto a pagar, para que su transacción sea tomada en cuenta por los mineros de la red.

En general, la ejecución de una transacción desempeña un papel fundamental dentro de la cadena de bloques y está relacionada con algunas variables esenciales al momento de desarrollar un proyecto descentralizado sobre la red *P2P*. Primero, considerar el uso de la red en el momento de enviar una transacción, es decir, su costo varía dependiendo de la congestión de la red en determinado momento. La figura 3.1 indica un gráfico de las transacciones pendientes, durante la semana del 25 al 29 de septiembre. Se tomó como escenario de prueba la red pública de *Blockchain*. Es evidente que las transacciones fluctúan variablemente en función del *GAS*, que está dado en unidades de Gwei.

Figura 3.1 Variación de la transacción en función de la congestión de la red[47].

[47] Información tomada de https://etherscan.io el día 30 de abril del 2018, a las 10H32.

Se realizaron 10 pruebas de transacciones, en la red principal, *Main Net* y KOVAN[48], mediante las carteras de *MyEtherWallet*[49] y *Etherscan*, los resultados se encuentran en el Anexo XV. A continuación, se va a presentar una prueba en cada red, con su respectivo análisis de resultados.

La figura 3.2 indica una prueba con la red principal. Al enviar 0.1 ETH, cuando existen 6015 transacciones pendientes y 38 *peers* conectados. Se prueba un *gas* de 21 Gwei y *Gas limit* de 2100. Dependiendo del ajuste que se realice a los parámetros del Gas, va a variar el tiempo de confirmación de la transacción. En esta prueba, tan sólo con enviar *Ether* de una dirección a otra se ejecuta de esta manera el contrato inteligente.

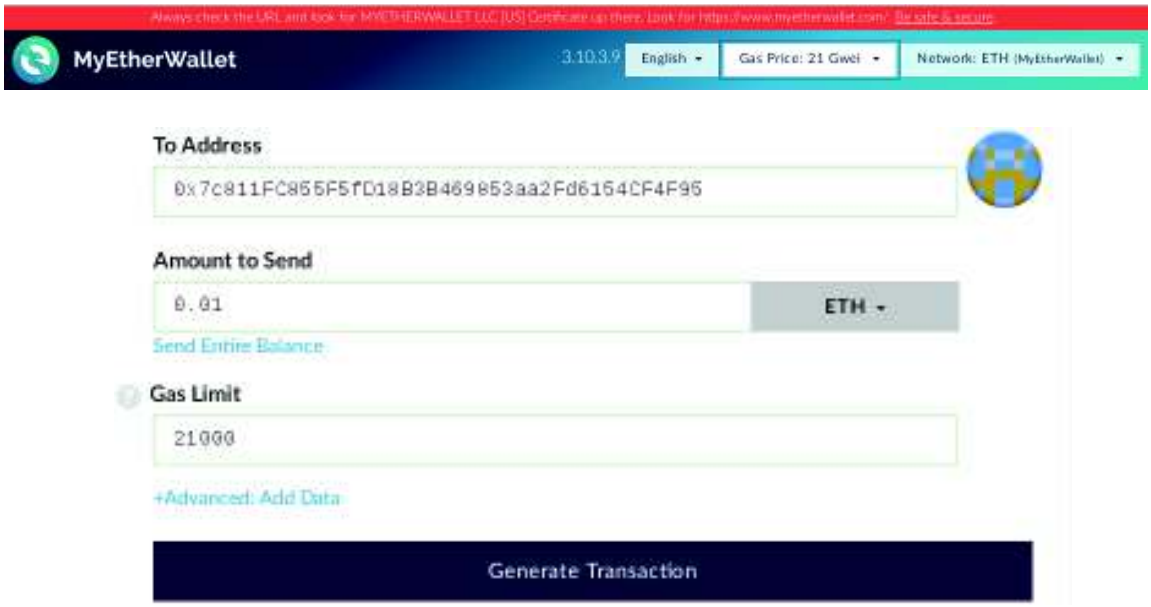

Figura 3.2 Transacción en la Red principal en *MyEtherWallet*[50]

En cambio, la figura 3.3 presenta la prueba que se realizó en la red de KOVAN al enviar 0.1 Ether, Cuando se realizó esta prueba, tan sólo existían dos transacciones pendientes y 60 *peers* conectados. Al momento de actualizar la página de *MyEtherWallet* el valor de las transacciones pendientes cambian constantemente, pero en ningún caso supera las 4 transacciones pendientes.

[48] KOVAN: Es una red de creada específicamente para desarrolladores, maneja su propio *token* KETH, disponible en su página oficial https://github.com/kovan-testnet/faucet
[49] *MyEtherWallet*: Cartera más utilizada por los usuarios de la plataforma *Ethereum*, para realizar transacciones.
[50] Información tomada de https://www.myetherwallet.com/ el día 30 de abril del 2018, a las 16H05.

Figura 3.3 Transacción en la Red de KOVAN en *Etherscan* [51]

De las pruebas realizadas durante el mes de abril y mayo, se analiza que el uso de la plataforma pública de *Ethereum* es inviable para un proyecto, donde el rápido envío de las transacciones de los eventos de emergencia es extremadamente crítico. El costo de la transacción es casi despreciable, lo que no encarece los gastos anuales por este servicio.

A la larga, la red pública resulta ser una opción cara y depende de la congestión de la red. Por lo tanto, si existen varias transacciones realizadas en el orden de 1000, implementando la red pública va a provocar que se generen algunas transacciones pendientes debido a la alta demanda de la red que realicen los otros usuarios.

Análisis del *token* ERC20

Se va a proceder a crear del *token* ERC20 para la aplicación descentralizada del sistema de alarmas residenciales sobre la plataforma de *Ethereum*, considerando los siguientes pasos:

- La figura 3.4 indica la cuenta 0xB8eD4….75 y su respectiva clave privada encriptada, donde se van a almacenar los *tokens* del sistema de alarmas. Se usa la página oficial de *MyEtherWallet* https://www.myetherwallet.com/#view-wallet-info para crear la cuenta.

[51] Información tomada de https://etherscan.io el día 3 de mayo del 2018, a las 15H30.

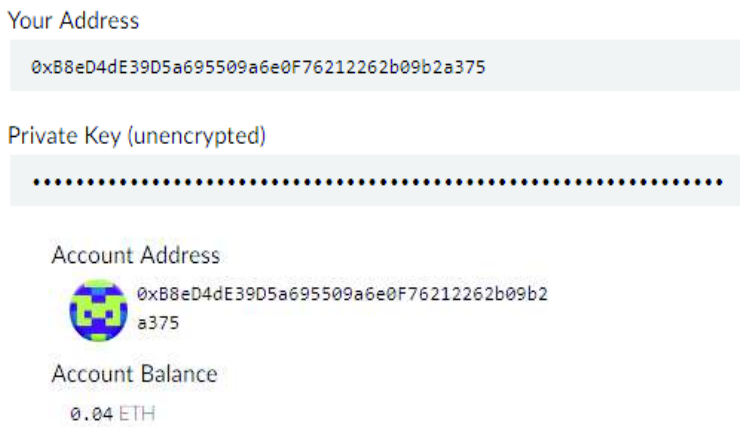

Figura 3.4 Cuenta para almacenar los *tokens*

- Se crea el *token* digital sobre la red privada *Blockchain*, basada en *Solidity,* que va a correr en la plataforma *Ethereum* para la aplicación descentralizada del sistema de alarmas residenciales. De esta manera, se van a transferir los eventos que van a ser compartidos en toda la red bajo el estándar ERC20.

```
1   pragma solidity ^0.4.20;
2
3   contract TokenERC20 {
4       /* Variables publicas del token */
5       string public standard = 'Token 0.1';
6       string public name;
7       string public symbol;
8       uint8 public decimals;
9       uint256 public initialSupply;
10      uint256 public totalSupply;
11
12      /* Creacion del array para el balance */
13      mapping (address => uint256) public balanceOf;
14      mapping (address => mapping (address => uint256)) public allowance;
15
16      /* Inicializacion del contrato con  tokens */
17      function TokenERC20() {
18          initialSupply = 1000000;
19          name ='SistemaAlarmasResidenciales';
20          decimals = 0;
21          symbol = 'SARToken';
22
23          balanceOf[msg.sender] = initialSupply;
24          totalSupply = initialSupply;
25      }
26
27      /* Enviar tokens */
28      function transfer(address _to, uint256 _value) {
29          if (balanceOf[msg.sender] < _value) throw;           // Revisa si hay tokens
30          if (balanceOf[_to] + _value < balanceOf[_to]) throw; // Chequea el overflow
31          balanceOf[msg.sender] -= _value;
32          balanceOf[_to] += _value;
33      }
34
35      /* Funcion cuando alguien trate de enviar ether */
36      function () {
37          throw;     // Prevee accidentalmente el envio de ether
38      }
39  }
```

Figura 3.5 Código del Token ERC20 en Solidity

- ERC20 permite la compatibilidad con cualquier otra *wallet* o contrato inteligente que use el mismo estándar. Se usa la página https://www.proofsuite.com/smartcontract/ para crear el contrato inteligente, como se indica en la figura 3.5. Se crean un millón de tokens para el Sistema de Alarmas Residenciales.
- Para compilar el contrato inteligente, se usa el browser de *Solidity,* https://ethereum.github.io/browser-solidity/#optimize=false&version=soljson-v0.4.24+commit.e67f0147.js Esta interfaz nos indica si el *Token*, SARCoin, cumple con las normas del estándar ERC20. Esta herramienta también trabaja con *Metamask*, que nos va permitir correr el contrato inteligente mediante la interfaz *Injected Web3*, como se muestra en la figura 3.6

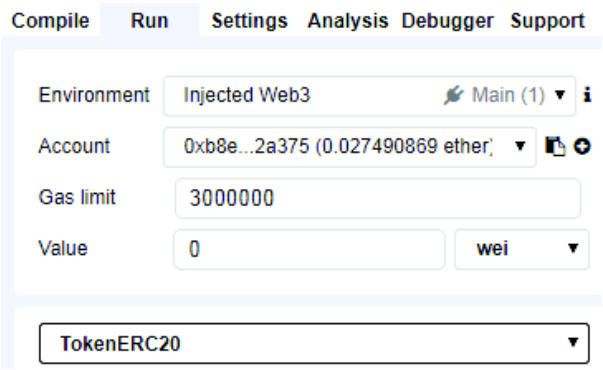

Figura 3.6 Compilación del contrato inteligente con la interfaz Injected Web3

- Para crear el *Smart contract* hay que confirmar la transacción. De acuerdo con las pruebas que se realizó para el Gas Price, que se detallan en el Anexo XVI, se considera el *Gas Price* de 7, más conveniente para este token. La figura 3.7 indica la confirma el contrato inteligente mediante el Metamask.

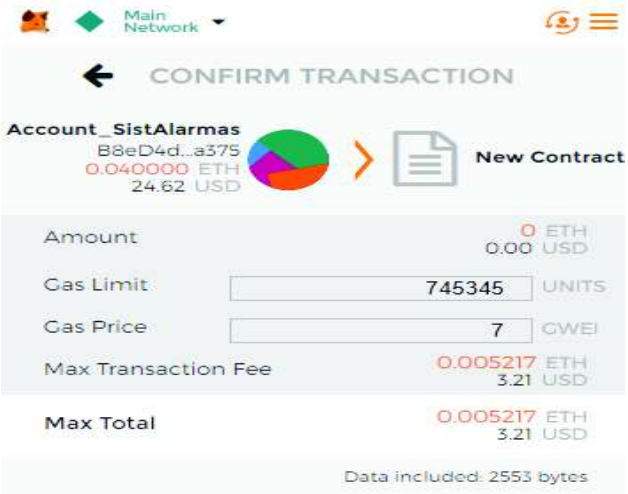

Figura 3.7 Confirmación del contrato en *Metamask*

- En cambio, la figura 3.8 muestra la ejecución del contrato en Etherscan https://etherscan.io con una confirmación de la transacción en 29 segundos. De esta forma, se comprueba la dirección del contrato que fue creado exitosamente.

Transaction Information

TxHash:	0x559608d2902ec63a650d2f64eea57f71fbf647cc1575af711a7d2aa3a4eee252
TxReceipt Status:	Success
Block Height:	5726264 (1 block confirmation)
TimeStamp:	29 secs ago (Jun-03-2018 05:20:20 PM +UTC)
From:	0xb8ed4de39d5a695509a6e0f76212262b09b2a375
To:	[Contract 0x42956daaf0d04cda5a0bb9e970751c58bc15d2c8 Created]
Value:	0 Ether ($0.00)
Gas Limit:	745345
Gas Used By Txn:	745345
Gas Price:	0.000000007 Ether (7 Gwei)
Actual Tx Cost/Fee:	0.005217415 Ether ($3.21)
Nonce & {Position}:	0 | {68}

Figura 3.8 Confirmación del contrato inteligente en *EtherScan*

- Ahora se comprueba que el contrato generado se transmita a la de la red privada, que se creó en *MyEtherWallet*.

- En la cuenta 0x429….5d2c8 se va a guardar el millón de tokens para realizar las transacciones de los eventos, como se indica en la figura 3.9.

Token Contract Address

0x42956daaf0d04cda5a0bb9e970751c58bc15d2c

Token Symbol

SARCoin

Decimals

0

Save

Figura 3.9 Transferencia de *tokens SAR* a la red privada de *Ethereum*.

- Se procede a trabajar con el SAR*Token* dentro de la red privada de *blockchain*, se edita el archivo génesis de todos los mineros y nodos con la nueva dirección y balance que hace referencia al contrato inteligente como se indica en la figura 3.10

```
{
    "nonce": "0x0000000000000042",
    "mixhash":
"0x0000000000000000000000000000000000000000000000000000000000000000",
    "parentHash":
"0x0000000000000000000000000000000000000000000000000000000000000000",
     "extraData":
"0x4426c6f7175652047656e657369732d53697374416c61726d6173",
    "config": {
        "chainId": 42,
        "homesteadBlock": 0,
        "eip155Block": 0,
        "eip158Block": 0
    },
    "difficulty": "200000000",
    "gasLimit": "21000",
    "alloc": {
        "0x42956daAf0D04cda5A0bB9E970751C58bc15d2c8": { "balance":
"1000000" }
    }
}
```

Figura 3.10 Cuenta del contrato en el bloque génesis de la cadena de bloques

- Se inicia el bloque génesis en los dos mineros y en el nodo del RPI. La figura 3.11 muestra la ejecución del bloque génesis en el minero 1, además indica donde se está almacenando toda la base de datos en la cadena.

```
alexita@SisAlarmasMinero: ~/ChainSkills
alexita@SisAlarmasMinero:~/ChainSkills$ gedit genesis.json
alexita@SisAlarmasMinero:~/ChainSkills$ geth --datadir ~/ChainSkill
s/minero1 init genesis.json
INFO [06-03|12:08:35] Maximum peer count                       ETH=
25 LES=0 total=25
INFO [06-03|12:08:35] Allocated cache and file handles         data
base=/home/alexita/ChainSkills/minero1/geth/chaindata cache=16 hand
les=16
INFO [06-03|12:08:36] Writing custom genesis block
INFO [06-03|12:08:36] Persisted trie from memory database      node
s=1 size=195.00B time=23.554112ms gcnodes=0 gcsize=0.00B gctime=0s
livenodes=1 livesize=0.00B
INFO [06-03|12:08:36] Successfully wrote genesis state         data
base=chaindata                                        hash=3da276…4
529c0
INFO [06-03|12:08:36] Allocated cache and file handles         data
base=/home/alexita/ChainSkills/minero1/geth/lightchaindata cache=16
 handles=16
INFO [06-03|12:08:36] Writing custom genesis block
INFO [06-03|12:08:36] Persisted trie from memory database      node
s=1 size=195.00B time=77.293µs    gcnodes=0 gcsize=0.00B gctime=0s
livenodes=1 livesize=0.00B
INFO [06-03|12:08:36] Successfully wrote genesis state         data
base=lightchaindata                                     hash=3da
276…4529c0
```

Figura 3.11 Bloque génesis en el minero 1

- La inicialización y ubicación de la base de datos de toda la cadena del minero 2 se indica en la figura 3.12. Todos los mineros apuntan hacia la dirección de almacenamiento de toda la cadena, es decir en la carpeta ***ChainSkills***.

```
SisAlarmasMinero: ~/Chainskills/minero2                    8:18 PM
alexita@SisAlarmasMinero:~$ cd ~/Chainskills
alexita@SisAlarmasMinero:~/Chainskills$ geth --datadir ~/Chainskills/
minero2 init genesis.json
INFO [05-22|20:18:21] Maximum peer count                       ETH=25
 LES=0 total=25
INFO [05-22|20:18:21] Allocated cache and file handles         databa
se=/home/alexita/Chainskills/minero2/geth/chaindata cache=16 handles=
16
INFO [05-22|20:18:21] Writing custom genesis block
INFO [05-22|20:18:21] Persisted trie from memory database      nodes=
0 size=0.00B time=6.586µs gcnodes=0 gcsize=0.00B gctime=0s livenodes=
1 livesize=0.00B
INFO [05-22|20:18:21] Successfully wrote genesis state         databa
```

Figura 3.12 Bloque génesis en el minero 2

- En el nodo del RPI se usa el comando geth y se ejecuta el mismo bloque génesis como se muestra en la figura 3.13.

```
pi@SistAlarmasNodo1: ~/ChainSkills
File  Edit  Tabs  Help
pi@SistAlarmasNodo1:~ $ cd ~/ChainSkills
pi@SistAlarmasNodo1:~/ChainSkills $ geth --datadir ~/ChainSkills/nodo init gen
is.json
INFO [05-01|22:04:03] Maximum peer count                       ETH=25 LES=0 to
l=25
INFO [05-01|22:04:03] Allocated cache and file handles         database=/home/
/ChainSkills/nodo/geth/chaindata cache=16 handles=16
INFO [05-01|22:04:04] Writing custom genesis block
INFO [05-01|22:04:04] Persisted trie from memory database      nodes=0 size=0.
B time=10.52µs gcnodes=0 gcsize=0.00B gctime=0s livenodes=1 livesize=0.00B
INFO [05-01|22:04:04] Successfully wrote genesis state         database=chaind
a                                hash=274f18…fa200b
INFO [05-01|22:04:04] Allocated cache and file handles         database=/home/
/ChainSkills/nodo/geth/lightchaindata cache=16 handles=16
INFO [05-01|22:04:04] Writing custom genesis block
INFO [05-01|22:04:04] Persisted trie from memory database      nodes=0 size=0.
B time=10.781µs gcnodes=0 gcsize=0.00B gctime=0s livenodes=1 livesize=0.00B
INFO [05-01|22:04:04] Successfully wrote genesis state         database=lightc
```

Figura 3.13 Bloque génesis en el nodo del RPI

- Se realiza las pruebas de sincronización entre los mineros y el nodo. Para sincronizar los mineros, primero deben conocerse sus pares para poder transmitir, de forma manual se debe configurar cada nodo para especificar la identidad y ubicación de sus *peers*.

- La figura 3.14 indica la forma como averiguar la dirección IP del computador que está corriendo los mineros, usando el comando ipconfig y poner la interfaz respectiva. El mismo procedimiento se sigue para el nodo.

```
alexita@SisAlarmasMinero: ~
alexita@SisAlarmasMinero:~$ ifconfig ens33
ens33     Link encap:Ethernet  HWaddr 00:0c:29:26:ae:0a
          inet addr:192.168.100.157  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: 2800:bf0:143:df9:e39b:daea:22d:7158/64 Scope:Global
          inet6 addr: fe80::4fdc:9536:bbc7:4e4c/64 Scope:Link
          inet6 addr: 2800:bf0:143:df9:90af:4041:61d0:f9a7/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:160820 errors:13 dropped:60 overruns:0 frame:0
          TX packets:93190 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:140943143 (140.9 MB)  TX bytes:17362005 (17.3 MB)
          Interrupt:19 Base address:0x2000
```

Figura 3.14 Dirección IP del minero en la red *Ethereum*

- Ahora, se actualiza el archivo static-nodes.json con la información de los mineros y nodo, añadiendo su respectiva dirección IP y puerto.

- Finalmente, para probar la sincronización de los participantes de la red se procede a transferir los tokens, por medio de la consola de Geth en JavaScript que se muestra en la figura 3.15. La figura 3.16, muestra las características del minero 1 con respecto a sus atributos de: dirección IP encriptada, la dirección remota de su vecino que está relacionada, la dificultad, versión, entre sus principales elementos. La figura 3.17, indica la relación del minero 1 que esta sincronizado con su par el minero 2, por medio de su puerto. La figura 3.18, indica la sincronización de los dos mineros con el nodo del RPI

```
alexita@SisAlarmasMinero: ~/ChainSkills
Welcome to the Geth JavaScript console!

instance: Geth/v1.8.6-stable-12683fec/linux-386/go1.10
 modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txp
ool:1.0 web3:1.0

> adminINFO [05-01|12:06:04] Upgrading chain index                    type=bloom
bits percentage=92
> admin.nodeInINFO [05-01|12:06:07] Finished upgrading chain index           typ
e=bloombits
> admin.nodeIndoINFO [05-01|12:06:08] Block synchronisation started
> admin.nodeInINFO [05-01|12:06:10] Imported new block headers               cou
nt=0 elapsed=19.954ms number=339354 hash=75a4bd…247da1 ignored=192
> admin.nodeInfoINFO [05-01|12:06:11] Imported new block receipts              c
ount=8 elapsed=1.178ms  number=339170 hash=da28eb…06c34e size=1.08kB ignored=0
```

Figura 3.15 Consola de Geth para la ejecucion del contrato en cada minero y nodo

```
[{
    caps: ["eth/63"],
    id: "ddb79194ca3057a74500d207aeae2f3c00c193c74ed016bc9375aec0bd6b11c7a45ee20
c0d905e9743622ac3ea1b220ea9a3ea010a86ed61ab2109fa41e32743",
    name: "Geth/v1.8.7-unstable-e7067be9/linux-amd64/go1.10",
    network: {
      inbound: false,
      localAddress: "192.168.100.157:59916",
      remoteAddress: "115.68.52.223:30303",
      static: false,
      trusted: false
    },
    protocols: {
      eth: {
        difficulty: 3.955290712733147e+21,
        head: "0x5f4ad1befb374ea2c825992d7def21b811e7aaf29ce75ed4390f70cbdbfc9b1
d",
        version: 63
      }
    }
```


Figura 3.16 Características del minero 1


```
    caps: ["eth/62", "eth/63"],
    id: "a00ff4f1e54eb051e20834345e05facf5d4b85feb82c732815f368f9477aeca9587ac8f
2da25525ea35cd4375be682f37a10eedceb915b393bceb9958753159",
    name: "Geth/v1.8.6-stable-12683fec/linux-amd64/go1.10",
    network: {
      inbound: false,
      localAddress: "192.168.100.157:42698",
      remoteAddress: "93.88.74.171:30303",
      static: false,
      trusted: false
    },
    protocols: {
      eth: {
        difficulty: 3.955433234674925e+21,
        head: "0xe5ad96d1fe7c79b8c545502d92aba34bad7b77d7062f47744f18f872c61121f
",
        version: 63
      }
    }
```


Figura 3.17 Sincronización entre los dos mineros


```
    caps: ["eth/62", "eth/63", "shh/2"],
    id: "e2f28126720452aa82f7d3083e49e6b3945502cb94d9750a15e27ee310eed6991618199
f878e5fbc7dfa0e20f0af9554b41f491dc8f1dbae8f0f2d37a3a613aa",
    name: "Geth/v1.5.3-stable-978737f5/linux/go1.7.3",
    network: {
      inbound: false,
      localAddress: "192.168.100.157:46496",
      remoteAddress: "139.162.13.89:55555",
      static: false,
      trusted: false
    },
    protocols: {
      eth: {
        difficulty: 36103006035539486000 0,
        head: "0x0ddc79111f878d4a77675739f2d13f52d51ad6f459b36df90c55d9ccbb171fc
2",
        version: 63
      }
    }
```


Figura 3.18 Sincronización entre los mineros con el nodo

- La figura 3.19 indica la sincronización de la cadena de bloques, mediante la interfaz de JavaScript.

```
alexita@SisAlarmasMinero: ~
Welcome to the Geth JavaScript console!

instance: Geth/v1.8.6-stable-12683fec/linux-386/go1.10
 modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txp
ool:1.0 web3:1.0

> INFO [06-03|19:40:51] Upgrading chain index                    type=bloombits
percentage=55
INFO [06-03|19:40:59] Upgrading chain index                    type=bloombits pe
rcentage=60
INFO [06-03|19:41:09] Upgrading chain index                    type=bloombits pe
rcentage=63
INFO [06-03|19:41:19] Upgrading chain index                    type=bloombits pe
rcentage=66
```

Figura 3.19 Actualización de la cadena de bloques

- La figura 3.20 muestra la transferencia del token en la cadena de bloques

```
alexita@SisAlarmasMinero: ~
> adminINFO [06-03|19:44:07] Imported new block receipts              count=256
 elapsed=63.810ms  number=752084 hash=93e6b8…33b67d size=677.23kB ignored=0
> admin.nodeInfoINFO [06-03|19:44:11] Imported new block receipts              c
ount=133  elapsed=37.746ms  number=752217 hash=a7c5b6…d8671b size=692.91kB ignor
ed=0
INFO [06-03|19:44:13] Imported new block headers              count=0    elapse
d=482.308ms number=765692 hash=e75bdb…6c0f8d ignored=1728
> admin.nodeInfo.INFO [06-03|19:44:14] Imported new block receipts
count=82   elapsed=17.091ms  number=752299 hash=6f6d7b…088851 size=443.96kB igno
red=0
> admin.nodeInfo.enode
INFO [06-03|19:44:19] Imported new block headers              count=0    elapse
d=44.792ms  number=766076 hash=3058e2…564961 ignored=384
INFO [06-03|19:44:19] Imported new block receipts              count=191  elapse
d=23.615ms  number=752490 hash=345512…031627 size=355.75kB ignored=0
"enode://7a59b5d09b73aa57d6b115f3b7eccd718e9a36fe5290d4d3a73514ff7c872faf517c452
0e7afbcc56dfb29773fbc0a8b6afd872183df22326a4410deb1fc262e@[::]:30303"
```

Figura 3.20 Importación de nuevos bloques recientes del minero

A pesar que dentro de la elaboración de este trabajo no está contemplado la implementación de la red privada *Ethereum*, se realizó la simulación de un contrato inteligente para crear el *token* del sistema de alarmas, llamado SARToken.

Si se incluye el mismo bloque génesis en toda la red *peer-to-peer,* con la dirección del contrato se puede transferir en toda la red el mismo *token,* ya que está diseñado con el estándar ERC20. Si se quisiera hacer comercial el *token* en la *CoinMarketCap* solo se necesita entrar en una subasta, *bid*, durante unas semanas, ya que el principio básico del estándar fue considerado para el contrato inteligente.

La figura 3.21 muestra la información de las direcciones de las cuentas relacionadas con los nodos dentro de la red P2P, con su respectivo número de *tokens* dentro del proyecto del sistema de alarmas mediante la interfaz de *Javascript.*

```
alexita@SistAlarmasMinero:~$ geth attach ~/.ethereum/geth.ipc
Welcome to the Geth JavaScript console!

instance: Geth/minero1/v1.8.11-stable-dea1ce05/linux-amd64/go1.10
coinbase: 0xb6567038ecaffe0da9d9af7c82c6410766d5714e
at block: 0 (Wed, 31 Dec 1969 19:00:00 -05)
 datadir: /home/alexita/ChainData/minero
 modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txp
ool:1.0 web3:1.0

> admin.nodeInfo.enode
"enode://58a5a6a288e2859bd0c6457975eee63c9a14a649fd39bfa7ec1b7c1bba526b71a81e333
2ee0f9cebf86fc9e5f741f55486d1cf0711e41b2382f9db0478e5f626@[::]:30303"
> personal.listAccounts
["0xb6567038ecaffe0da9d9af7c82c6410766d5714e", "0xc7750d0d4c263aa7788e89593e6544
42e8eb6947"]
> eth.getBalance(eth.accounts[0])
1.2089258196146291747061 76e+24
```

Figura 3.21 Información de las cuentas *peers* del nodo

La figura 3.22 indica los resultados de las transacciones que se realizaron entre los nodos de un computador y un nodo en el *Raspberry Pi*. Por seguridad de la cadena de bloques, antes de realizar la transacción primero es necesario desbloquear la cuenta con la respectiva contraseña cifrada, desde donde se origina la transferencia. Toda la cadena de bloques trabajo en la misma red privada Ethereum y con el mismo protocolo.

```
> personal.unlockAccount(eth.accounts[1], "estaeslacuenta#2Minero")
true
> eth.sendTransaction({from: eth.accounts[1], to: eth.accounts[0], value: web3.t
oWei(10, "ether")})
"0x173fa658d5c024fc38bf46c01fe49f3669b9bbb3ba93656e71fd75c8aff05f86"
INFO [07-02|23:36:06] Disk storage enabled for ethash DAGs     dir=/home/alexita/.ethash
                      count=2
INFO [07-02|23:36:06] Initialising Ethereum protocol           versions="[63 62]" networ
k=42
INFO [07-02|23:36:06] Loaded most recent local header          number=0 hash=aac069…8b28
b7 td=1024
INFO [07-02|23:36:06] Loaded most recent local full block      number=0 hash=aac069…8b28
b7 td=1024
INFO [07-02|23:36:06] Loaded most recent local fast block      number=0 hash=aac069…8b28
b7 td=1024
INFO [07-02|23:36:06] Regenerated local transaction journal    transactions=0 accounts=0
INFO [07-02|23:36:06] Starting P2P networking
INFO [07-02|23:36:08] UDP listener up                          self=enode://58a5a6a288e2
859bd0c6457975eee63c9a14a649fd39bfa7ec1b7c1bba526b71a81e3332ee0f9cebf86fc9e5f741f55486d1
cf0711e41b2382f9db0478e5f626@[::]:30303
INFO [07-02|23:36:08] RLPx listener up                         self=enode://58a5a6a288e2
859bd0c6457975eee63c9a14a649fd39bfa7ec1b7c1bba526b71a81e3332ee0f9cebf86fc9e5f741f55486d1
cf0711e41b2382f9db0478e5f626@[::]:30303
INFO [07-02|23:36:08] IPC endpoint opened                      url=/home/alexita/.ethere
um/geth.ipc
INFO [07-02|23:37:39] Etherbase automatically configured       address=0xB6567038ecAfFE0
da9d9AF7c82C6410766D5714E
INFO [07-03|00:17:43] Submitted transaction                    fullhash=0x173fa658d5c024
fc38bf46c01fe49f3669b9bbb3ba93656e71fd75c8aff05f06 recipient=0x86567038ecAfFE0da9d9AF7c8
2C6410766D5714E
```

Figura 3.22 Transferencia de *tokens* desde los mineros en la red P2P

Al momento que se genera la transacción, esta es enviada a todos los miembros de la red P2P. Una vez que los nodos escuchan se propagada al resto y empieza el proceso de minado como se muestra en la figura 3.23.

```
INFO [07-03|00:17:43] Submitted transaction                    fullhash=0x173fa658d5c024
fc38bf46c01fe49f3669b9bbb3ba93656e71fd75c8aff05f86 recipient=0xB6567038ecAfFE0da9d9AF7c0
2C6410766D5714E
INFO [07-03|00:17:43] Commit new mining work                  number=1143 txs=1 uncles=
0 elapsed=2.000s
INFO [07-03|00:17:49] Successfully sealed new block           number=1143 hash=dfeb21…d
948db
INFO [07-03|00:17:49] block reached canonical chain           number=1138 hash=45af9e…1
2f4a5
INFO [07-03|00:17:49] mined potential block                   number=1143 hash=dfeb21…d
948db
INFO [07-03|00:17:49] Commit new mining work                  number=1144 txs=0 uncles=
0 elapsed=142.734µs
```

Figura 3.23 Proceso de minado de una transacción

El proceso de minado de esta nueva transacción está a cargo del minero. La sincronización de los nodos de la red se realiza en segundos. Además, paulatinamente los nodos realizan el descubrimiento de sus vecinos que conversan el mismo lenguaje, sincronizando en el *ledger* una copia de la transacción en cada nodo, en todo momento la información se mantiene encriptada sobre toda la red para mantener su anonimato.

La configuración de los nodos permite realizar las transacciones del *token* ERC20 en el sistema de alarmas sobre la red P2P. El monedero permite administrar las cuentas y compilar el contrato inteligente del sistema de alarmas que esta sincronizado con la *Blockchain* privada.

La figura 3.24 muestra el acceso remoto hacia la interfaz de *Javascript* del RPI para comprobar la dirección de la cuenta del nodo. Además, se procede a comprobar los tokens que tiene la cuenta que son 0 porque no se produce aún ninguna transacción.

```
alexita@SlstAlarmasMinero:~$ ssh pi@192.168.100.147
pi@192.168.100.147's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jul  3 00:02:07 2018 from 192.168.100.160
pi@SlstAlarmasNodo:~ $ geth attach
Welcome to the Geth JavaScript console!

instance: Geth/nodo1/v1.8.1-stable-1e67410e/linux-arm/go1.9.4
coinbase: 0xc1caa724f2b085cf56c6c9ccb2b5a1f4946bb38b
at block: 0 (Wed, 31 Dec 1969 19:00:00 -05)
 datadir: /home/pi/ChainSkills/nodo
 modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txp
ool:1.0 web3:1.0

> personal.listAccounts
["0xc1caa724f2b085cf56c6c9ccb2b5a1f4946bb38b", "0xfef834ef18790f2aa0a26447c8379d
> eth.getBalance(eth.accounts[0])
0
```

Figura 3.24 Acceso remoto a la cuenta del nodo en el RPI

La figura 3.25 indica la transferencia de la transacción de 100 *tokens* desde el minero hacia el nodo del RPI. En este proceso el minero desbloque la cuenta y apunta hacia la dirección donde se van a transferir los *tokens*, es decir, la cuenta del nodo en el RPI. Procede a realizar el proceso de minado que toma unos segundos.

```
> personal.unlockAccount(eth.accounts[0], "estaeslacuenta#1Minero")
true
> eth.sendTransaction({from: eth.accounts[0], to: "0xc1caa724f2b085cf
56c6c9ccb2b5a1f4946bb38b", value: web3.toWei(100, "ether")})
"0x3dabfb89dd3a0fd31f9c6499d1510e6356742df76d66f897f9a23a17a35e4bc9"

INFO [07-03|00:39:02] Submitted transaction                    fullhash=0x3c
abfb89dd3a0fd31f9c6499d1510e6356742df76d66f897f9a23a17a35e4bc9 recipient=0xc
1CaA724F2B085cF56c6c9ccb2b5A1f4946BB38b
INFO [07-03|00:39:02] Successfully sealed new block            number=1778
ash=4e0e93…4e5338
INFO [07-03|00:39:02] Block reached canonical chain            number=1773
ash=3a3c02…159b2e
INFO [07-03|00:39:02] Mined potential block                    number=1778
ash=4e0e93…4e5338
INFO [07-03|00:39:02] Commit new mining work                   number=1779
txs=1 uncles=0 elapsed=350.141µs
INFO [07-03|00:39:09] Successfully sealed new block            number=1779
ash=9433d7…801ecb
```

Figura 3.25 Transferencia de *tokens* desde del minero hacia el nodo

Finalmente, la figura 3.26 muestra la verificación de la transferencia de 100 *tokens* del sistema de alarmas hacia la cuenta del RPI desde el minero. Mismo proceso se realiza en la cuenta del nodo del RPI, donde se comprueba que la misma cantidad de tokens han sido acreditados a esa cuenta. Por lo tanto, el tiempo de transferencia de una transacción es casi instantáneo, se conserva el anonimato del usuario y el proceso se desarrolla en un ambiente seguro y eficiente.

```
alexita@SistAlarmasMinero: ~
> web3.fromWei(eth.getBalance("0xc1caa724f2b085cf56c6c9ccb2b5a1f4946b
b38b"))
100

pi@SistAlarmasNodo: ~
> eth.getBalance(eth.accounts[0])
100
```

Figura 3.26 Transferencia de *tokens* desde el minero hacia el nodo

Al momento de correr la cadena de bloques de la plataforma *Ethereum* en otra red, puede que al principio el proceso de sincronización entre los pares y las cuentas demande un tiempo de espera de algunos minutos. Este inconveniente se produce debido a las restricciones de la nueva red ya sea por la congestión o el firewall impide su comunicación. Otro inconveniente para sincronizar la cadena de bloques se genera por la comunicación entre los nodos a través del número de puerto, que puede estar asignado a otra aplicación si se ejecuta el sistema de alarmas descentralizado en otra red doméstica o privada.

3.2. Análisis del sistema de alarmas residenciales tradicional y con la tecnología *Blockchain* (centralizado/descentralizado)

Hoy en día, la mayoría de empresas de monitoreo de sistemas de alarmas tradicionales no responden las necesidades de los usuarios, por ejemplo, demandan un costo continuo por este servicio y el tiempo de respuesta de atención al evento puede involucrar varios minutos. Por otra parte, algunas veces el personal de seguridad no está correctamente calificado o se encuentra fuera del sector de cobertura ante una emergencia. En otros casos, los datos del cliente pueden estar expuestos fácilmente, como en cualquier sistema centralizado.

Generalmente, la empresa de seguridad es la encargada de brindar el servicio de monitoreo a los usuarios. Dependiendo de sus requerimientos el costo de este servicio puede variable, así como, la calidad del mismo. En los sistemas centralizados, la central receptora es la encargada de controlar, supervisar y realizar el mantenimiento del sistema. Además, si se genera un evento de emergencia, esta se encarga de comunicarse con el propietario, personal del UPC o bomberos en función del tipo de alarma. Por lo tanto, al ser un modelo dependiente de una empresa, el usuario en ningún momento tiene control del sistema, simplemente sabrá que ocurrió un evento si accede a alguna aplicación o página web.

Normalmente, en los sistemas de monitoreo convencionales existe un intermediario o una entidad centralizada que registra y controla los eventos. De esta manera, el servidor representa un punto crítico para el sistema de alarmas. En cambio, con la tecnología *Blockchain,* la gestión de los eventos de alarma se realiza de forma independiente entre todos los nodos que conforman la red. El número de nodos es proporcional al número de casas que cuentan con el sistema de alarmas y el presentante de la UPC. Los mineros (computadoras personales) y nodos (*Raspberry Pi)*, se conectan a la red *peer-to-peer* para propagar los eventos en tiempo real.

Considerando los sistemas de alarmas residenciales basados en la cadena de bloques, se evitará depender de un computador central para la supervisión de los eventos y se eliminará la posibilidad de un único punto de falla. Por lo tanto, cada nodo mantiene copias de todo el historial de eventos y son almacenados cronológicamente en una base de datos, *ledger*, distribuida a través de Internet. Cada bloque se concatena uno a uno por medio de sus *hashes*.

En *Blockchain,* el *token* o activo digital hace que el sistema sea distribuido y completamente descentralizado. De esta manera, los sistemas descentralizados proporcionan seguridad y eficiencia en su servicio. La red antes de aceptar una transacción como válida realiza unos procesos previos, por ejemplo, los mineros son los encargados de realizar la prueba de trabajo implementando el algoritmo de consenso.

La tecnología *Blockchain* proporciona transparencia, confianza, seguridad e integridad de los datos para cada usuario que forma parte de la red *peer-to-peer*. La tabla 3.1 muestra un cuadro con las características para la gestión de la información del sistema de alarmas tanto en el caso tradicional como con la nueva tecnología *Blockchain*. Por lo tanto, se puede analizar las ventajas y desventajas de la gestión de la información del sistema de alarmas tradicional y en el sistema de alarmas con la nueva tecnología *Blockchain*.

Tabla 3.1 Cuadro de la gestión de la información del Sistema de Alarmas Tradicional vs la Tecnología *Blockchain*

	Sistema de Alarma Tradicional	**Sistema de Alarma Moderno con Tecnología *Blockchain***
Topología	Centralizado en bus	Descentralizado en una Red Punto a punto - P2P
Monitoreo	Depende de una empresa que brinde este servicio. Monitoreo 24 horas, los 7 días de la semana durante todo el año. Costo es mensual	No existe una empresa que realice el monitoreo. Protección 24 horas, los 365 días del año.
Elementos:	Central receptora de alarmas (CRA) Panel de alarmas Sensores y detectores Botones de pánico Teclado numérico Sirena	Panel de alarmas Sensores y detectores Botones de pánico Teclado numérico Sirena Raspberry Pi 3 PC
Estructura	Base de datos	Cadena de bloques – Transacciones - *Ledger*
Mecanismo de seguridad	El proveedor alerta al UPC que se ha producido una emergencia.	La UPC actúa directamente ante un evento de emergencia. Participación de la comunidad en su propia seguridad.
Tiempo de respuesta	En cuestión de minutos	En razón de segundos
Algoritmo	No tiene	SHA-256
Consenso	No trabaja	Prueba de Trabajo - PoW
Plataforma	No utiliza	*Ethereum*

En el Sistema de Alarmas Tradicional presenta las siguientes ventajas:

- Fácil uso y formación para el personal que realice el mantenimiento.
- Dispone de personal para brindar la seguridad en caso de intrusión.

Pero el sistema convencional de alarmas presenta algunas desventajas:

- Sistema centralizado es vulnerable ya que depende del correcto funcionamiento de la unidad central.
- Depende de la empresa que maneja la central receptora de alarma (CRA) para controlar y supervisar la gestión de los eventos.
- El tiempo de respuesta en muchos casos conlleva más que unos minutos.

Con respecto al Sistema de alarmas mediante la Tecnología *Blockchain* se presentan algunas ventajas:

- Cuenta con una topología descentralizada, donde todos los miembros de la red P2P manejan la información de los eventos; con claridad y precisión todos los usuarios sabrán la cantidad de alarmas ocurridas y si hay relación con el tiempo de respuesta de la policía.
- La confianza de la gestión de la información se consolida por el algoritmo de consenso y el estándar ERC20.
- La tecnología *Blockchain* al manejar en su estructura la cadena de bloques, asegura que la información que se encuentra en el *ledger* no es susceptible al sabotaje o manipulación de la información.
- No requiere una central de monitoreo para la gestión de los eventos, la tecnología *Blockchain* trabaja con cadenas de bloques que se encuentran distribuidas en todos los nodos de la red.
- Existe una comunicación directa con los miembros de la UPC, así como también con los vecinos cercanos que forman el *peer*, quienes podría dar asistencia y actuar más rápido ante una señal de intrusión.
- Elimina la necesidad de contratar intermediarios para el monitoreo y seguridad, lo que reduce los posibles puntos de falla.
- Facilita la posibilidad de la ampliación de la red con un reducido cableado y sin tanto papeleo.
- Los principios de la tecnología *Blockchain* se pueden implementar en la plataforma *Ethereum* que trabaja con *Smart Contracts* y *PoW* para brindar seguridad a la red.

A continuación, se indican algunas desventajas con respecto a la implementación de la tecnología *Blockchain* en los sistemas de alarmas:

- Se mantiene aún en cierta parte del sistema de alarmas, un dispositivo centralizado (Panel de alarmas) que recibe todos los eventos, como tal puede ser vulnerable.
- El personal técnico para instalar, configurar y realizar el mantenimiento requiere un mayor entrenamiento que en el sistema tradicional.
- Como un proyecto a futuro *Ethereum* implementará *PoS,* para mejorar la PoW y de esta forma reducir el procesamiento computacional para ser más amigable con el medio ambiente.
- Requiere en ocasiones mayor complejidad en la programación de la cadena o contrato inteligente.
- Según el tipo de *Dapp* que se realice va a requerir un mayor o menor gasto energético. En este caso de los eventos que son enviados por las salidas programables del panel, esta información no involucra mayor coste computacional que en un sistema financiero.

De lo anterior expuesto existen grandes ventajas en los sistemas de alarmas con incursión de la tecnología *Blockchain* con respecto al sistema convencional.

De esta manera, dentro del contexto definido para los sistemas de alarmas descentralizados, los miembros de la comunidad cuenten con mineros que van a calcular la PoW más rápido y van a recibir algún tipo de recompensa por su contribución computacional. De esta forma se evita la necesidad de depender de algún intermediario para la validación de la información, con lo cual se reduce el riesgo de error humano.

Actualmente, el sistema de alarmas tradicional tiene una comunicación directa con la central de monitoreo a través de las líneas telefónicas, si se produce un corte en la línea no se podrán transmitir los eventos al servidor y la empresa no aplicará el protocolo de emergencia, es decir, el sistema solo funcionará localmente activando la sirena Este inconveniente se soluciona con la cadena de bloques, ya que a través de las salidas programas del panel de alarmas los eventos son transmitidos autónomamente a través de la red P2P a todos los nodos. Por otro lado, si cae un nodo, el resto mantiene una copia de la información, de esta forma, se mantiene la sincronización de los eventos entre todos los miembros de la comunidad. El tiempo de respuesta ante una emergencia depende de la propagación de la cadena de bloques sobre Internet.

3.3 Análisis de Costos

La tabla 3.2 muestra un análisis comparativo del costo del sistema de alarmas tradicional y con la Tecnología *Blockchain*. Se va a considerar en el análisis de costos anual de las 30 casas. La implementación de un sistema de alarmas cableado en el mercado, ofrece mayores beneficios de seguridad, pero implica mayor costo en la mano de obra. Considerando este punto, en ambos sistemas de alarmas, para la comparación del análisis el costo de los equipos e instalación, no se va a considerar esto para esta parte.

Tabla 3.2 Análisis de costos para la gestión de la información del sistema de alarmas tradicional y con la Tecnología *Blockchain*

Tipos de Costos	Sistema de alarmas tradicional	Sistema de alarmas Moderno con Tecnología *Blockchain*
Monitoreo	$ 9,990.00	
Mantenimiento	$ 0.00	$ 53.84
Hardware y accesorios para mineros y nodos		$ 3,011.1
Instalación del software para la red P2P		$ 149.92
Implementación de la red *Ethereum* Privada		$ 1,033.30
TOTAL	**$ 9,990.00**	**$ 17,404.36**

Para el costo del hardware y accesorios adicionales en la red P2P, se supone que existe un PC que cumple con los requerimientos mínimos para los mineros; entonces sólo se va a considerar el costo de los nodos. No existe costo de operación debido a que la tecnología *Blockchain* no necesita de intermediarios para el funcionamiento de la red, pero si involucra un gasto de implementación para el minero, nodo y contrato inteligente.

Al analizar el coste global anual de las 30 casas en el sistema de alarmas tradicional asciende $**9,990.00**, mientras que con el sistema moderno considerando los 30 nodos y los 4 mineros es de **$ 17,404.36**. A simple vista, el sistema de alarmas convencional implica un menor costo para el usuario. Pero si se analiza detenidamente durante los siguientes años, este sería sólo un beneficio momentáneo que tendrían los usuarios.

La tabla 3.3 indica el análisis de costos de los dos sistemas de alarmas, centralizado y descentralizado, durante tres años. El primer año, el usuario por contar con un sistema de seguridad ante intrusos con la tecnología *Blockchain*, debe cancelar un costo adicional de hardware y software para los mineros y nodos de la red. Este gasto encarece el servicio en el primer año, con respecto al sistema de alarmas que depende de una empresa para su

funcionamiento. En los siguientes años, los usuarios ya no deben cancelar ese valor. La cadena de bloques con lleva un ahorro en este servicio debido a su independencia y autonomía.

Tabla 3.3 Análisis de costos anual de los sistemas de alarmas

Tipo de sistema de alarmas	Año 1	Año 2	Año 3
Sistema Centralizado (Tradicional)	$ 9,990.00	$ 9,990.00	$ 9,990.00
Sistema Descentralizado (*Blockchain*)	$ 17,404.36	$ 53.84	$ 53.84

Al ser una tecnología nueva y no tener ninguna aplicación descentralizada antecesora en este ámbito, en sus primeros años de vida, necesita del servicio de mantenimiento por parte de un técnico. Si se compara este costo de mantenimiento con el coste de monitoreo, representa un alto valor que anualmente todos los usuarios deben cancelar por este servicio a una empresa, como ocurre en el sistema tradicional.

A los dos años, las 30 casas pagarían a la operadora del monitoreo **$ 19,980.00**; mientras que en el primer año con *Blockchain,* la comunidad sólo pagaría **$ 17,404.36,** lo que ahorro del 26%. Si se considera los siguientes años, el ahorro es mayor ya que cada usuario ya no cancelaría el costo del hardware, instalación ni implementación. La confiabilidad y seguridad de la gestión de la información de los eventos con la tecnología *Blockchain* es transparente para todos los miembros de la red, sin necesidad de depender o confiar del servicio por parte de una empresa.

Al contrastar el cuadro de los costos, se puede apreciar que el sistema de alarmas considerando la cadena de bloques, es más conveniente para el usuario, lo que presenta un ahorro de **$ 2,575.64** para todos los usuarios, en el segundo año; en el resto de años el ahorro es de **$ 9,936.16**, lo que equivale casi al 100%. Además, la confiabilidad y seguridad de la gestión de la información de los eventos con la tecnología *Blockchain* es transparente para todos los miembros de la red, sin necesidad de depender o confiar del servicio por parte de una empresa.

4. CONCLUSIONES

- Ecuador apunta a la innovación e incorpora en uno de sus ejes estratégicos el desarrollo de nuevas tecnologías. *Blockchain* se basa en un sistema descentralizado que busca solucionar los problemas que brindan los modelos centralizados, tanto así que, la cadena de bloques generaría valor al desarrollo social y económico de nuestro país.

- Particularmente, la cadena de bloques en los sistemas de alarmas residenciales elimina la necesidad de depender de un servidor central, tal como ocurre en los actuales sistemas de alarmas. La gestión de los eventos se produce a través de las salidas programables del panel, como, botón de pánico, eventos de emergencia y sirena, que son transferidas hacia las entradas GPIO del *Raspberrry* Pi.

- La cadena de bloques proporciona a los miembros de la comunidad un sentido de bienestar ante una situación de emergencia con una disponibilidad del servicio las 24 horas del día y sin un costo mensual. Esto mejoraría la productividad y calidad de vida de los usuarios respecto a los avances digitales.

- Los sistemas de alarmas residenciales en el modelo descentralizado constituyen una herramienta eficiente y segura. Las transacciones se registran públicamente en la base de datos distribuida o *ledger*, para que no exista la posibilidad que ningún miembro de la red pueda modificar o alterar la información. Por lo tanto, la transacción es almacenada cronológicamente dentro de la cadena de bloques y en tiempo real.

- La cadena de bloques se encuentra presente en cada uno de los nodos y se actualiza cada tiempo con la generación de un evento, en la simulación la actualización del nuevo bloque tomó unos pocos segundos. Los bloques se construyen con relación al hash anterior. Este proceso brinda la confidencialidad e integridad a la información sin depender de una empresa centralizada.

- La tecnología *Blockchain* protege la información de todos los miembros sobre la red P2P. Cuenta con varios mecanismos de seguridad relacionados con el bloque génesis y el hash del bloque, así como, las direcciones encriptadas y la prueba de trabajo para auditar toda la cadena. Este proceso garantiza la transparencia y confiabilidad del sistema.

- *Blockchain* cuenta con varias plataformas distribuidas sobre Internet. Se destacan *Ripple,* e *IOTA*, cada una con sus propias características y beneficios; pero *Ethereum* encaja perfectamente en el alcance de este trabajo. Presenta un gran potencial para desarrollar nuevas aplicaciones descentralizadas con la ejecución autónoma de contratos inteligentes. Esto reduce el riesgo de fraudes, perdida de información y elimina la sumisión de terceras partes para contratar un servicio.

- Considerando la plataforma *Ethereum* para la simulación de la transferencia del token del sistema de alarmas, se analiza que este escenario no presenta mayores inconvenientes de latencia en la red y las transacciones pendientes generadas son mínimas. Esto se debe, a que el número de participantes en la red privada es reducido y con acceso restringido, por lo tanto, no existe demora en el servicio.

- En el presente estudio, la cadena de bloques se convierte en un mecanismo de ahorro económico para el mercado residencia local. Evidentemente en la red privada *Ethereum*, la transacción sería tomada en cuenta por la red de forma casi inmediata, ya que los costos de envío de información son prácticamente de $0.

- La inclusión de la tecnología *Blockchain* en los sistemas de alarmas residenciales presenta como ventaja el *backup* de las transacciones. Los eventos generados sobre la red *peer-to-peer* se sincronizan en todos los nodos, por lo tanto, brindan respaldo de toda la información. Este proceso reduce el riesgo de congestión de la red y garantiza la redundancia en todo el sistema.

- Los sistemas de alarmas tradiciones usan un servidor central para la gestión de los eventos, si se cae este, puede implicar la suspensión del servicio por algunas horas. En cambio, con la cadena de bloques esta situación no sucede, ya que cada nodo de la red P2P, reciben una copia de toda la cadena de eventos.

- El éxito del proyecto de los sistemas de alarmas descentralizados, depende de la organización y colaboración comunitaria. Además, los miembros de la red participan en el consenso de las alertas, de esta manera, contribuyendo responsablemente de la seguridad comunitaria y fortalecen sus lazos de convivencia. La participación de la policía juego un rol primordial para atender a un llamado de alerta en el menor tiempo posible.

- Los sistemas de alarmas convencionales, la información recolectada de las alarmas comunitarias no es segura, ya que depende del buen estado de las instalaciones hacia los puntos de administración, la comunicación de los eventos al UPC y conectividad del servidor WEB.

- Por otro lado, relacionando el costo del sistema de alarmas tradicionales versus la tecnología *Blockchain,* el gasto de monitoreo que mensualmente el usuario cancela y los beneficios que recibe por parte de la empresa proveedora no cubren sus demandas. En cambio, al comparar el sistema de alarmas mediante la cadena de bloques, este modelo requiere un menor gasto, presenta mayor confiabilidad en la gestión de la información y con un menor tiempo de respuesta ante una emergencia.

- Este presente estudio técnico sobre la tecnología *Blockchain* puede ser útil para trabajos futuros de investigación en la carrera sobre el Internet de las Cosas (*IoT*), Inteligencia Artificial e Big Data. Generalmente, se podría implementar para análisis de macrodatos, almacenamiento y transferencia de la información en la nube, conectividad, entre otras.

RECOMENDACIONES

- Para no causar algún tipo de conflicto con los datos almacenados que provienen de la *Blockchain* pública, es recomendable emplear una misma nomenclatura para almacenar dentro de una misma carpeta específica el directorio principal de la cadena de bloques, las cuentas y el monedero.

- Para la transferencia de transacciones, es recomendable asignar un adecuado valor de *Gas Limit* y *Gas Price* lo va a garantizar el envío y procesamiento de la información en la *Main Net* de *Blockchain.* Al momento de ejecutar el contrato inteligente depende directamente del gas que se asigne y el volumen de la información que se maneje sobre la red pública y cuyo valor también es variable.

- Mantener el mismo identificador de red, *network id*, en todos los nodos y mineros, asegura la sincronización de los datos en la red P2P. Además, antes de correr la red privada de *Blockchain*, es importante verificar que cada nodo de la red trabaje con el mismo archivo génesis en toda la cadena de bloques.

- Para trabajar con los eventos de las salidas programables del panel, es necesario instalar la librería de gpiozero en el RPI. Además, la señal del botón de pánico va a provenir de los pulsantes y es necesario adicionar un circuito extra con un relé y un diodo, para proteger el equipo y se disipe en ese elemento la corriente.

- En la simulación se verificó que, existen ciertos valores que están reservados (0-3) y no se pueden usar para configurar el identificador de la red. Además, al momento de instalar el nodo, se puede trabajar con el mismo número de puerto en dispositivos diferentes; pero, si se va a realizar la simulación en un solo computador es necesario configurar cada nodo con diferente número de puerto.

- Se recomienda emplear una contraseña robusta de más de 8 caracteres para configurar las cuentas. Es primordial familiarizarse con la contraseña ya que se maneja cada vez que se accede al monedero y cuentas.

- Es fundamental instalar todas las herramientas necesarias para manejar la consola de *Geth*, para configurar y sincronizar los nodos de forma interactiva. También es necesario comprobar la versión del geth que sea compatible con *Mist*, para evitar cualquier inconveniente al trabajar por consola de *JavaScript*.

- Tener en cuenta las reglas del estándar ERC20 para crear un token, facilita la comercialización del mismo en el mercado digital a través del CoinMarketCap.

- Para trabajar con el mismo bloque génesis entre los nodos y mineros de la red P2P, se puede transferir el archivo genesis.json de una manera dinámica mediante el comando sftp o remotamente con ssh mediante la dirección IP del respectivo nodo de acceso.

- Si existe algún inconveniente con las cuentas de los nodos o sincronización entre los pares de la red privada *Ethereum*, es recomendable verificar el archivo raíz de la cadena de bloques y el subdirectorio geth con la dirección /resources/node/geth/

5. REFERENCIAS BIBLIOGRÁFICAS

[1] L. Lezama, “Modelado de dispositivos para un sistema de seguridad implementando tecnología Jini,” Universidad de las Américas Puebla, 2001.

[2] M. Valera and S. A. Velastin, “Intelligent distributed surveillance systems,” *IEE Proc.-Vis. Image Signal Process.*, vol. 152, no. 1, pp. 192–204, 2005.

[3] “Estructura de una central de monitoreo de alarmas, topología y tendencias,” *TecnoSeguros*, 2012. [Online]. Available: https://www.tecnoseguro.com/tutoriales/alarma/estructura-de-una-central-de-monitoreo-de-alarmas-topologia-y-tendencias.html. [Accessed: 08-Nov-2017].

[4] “PC1616/PC1832/PC1864 versión 4.5. Guía de instalación,” 2011.

[5] DSC Power Series Security System, “PC1616/PC1832/PC1864. Guía de instalación,” 2007.

[6] “Conexión de linea telefónica en PC1832,” *Ilirey S.A*. 2016.

[7] “Sur-Gard System III Multi-Platform Digital Telephone Receiver,” *Digit. Secur. Control.*, vol. Version 1., p. 15, 2005.

[8] J. Ontiveros, “¿Cuales son los formatos más comunes de comunicación para centrales de monitoreo?,” *Tecnosinergia*, 2017. [Online]. Available: https://tecnosinergia.zendesk.com/hc/es/articles/360000632231--Cuales-son-los-formatos-mas-comunes-de-comunicación-para-centrales-de-monitoreo-. [Accessed: 25-Jun-2017].

[9] M. B. Merizalde, “Alarmas comunitarias frenan los delitos,” *El Comercio*, Quito, Jun-2017.

[10] “Tecnologia Blockchain,” *BBVA Innov. Cent. Fintech Ser.*, p. 25, 2016.

[11] W. Jane, A. Martin, and S. Philip, “Encadenados a Blockchain, la tecnología en la que se basa Bitcoin,” *Financial Times*, 2015. [Online]. Available: http://www.expansion.com/actualidadeconomica/2015/12/10/5669433d268e3eed3a8b4611.html. [Accessed: 07-Nov-2017].

[12] “GitHub is how people build software,” 2018. [Online]. Available: https://github.com/about. [Accessed: 27-Jul-2018].

[13] J. Cabezas, “Blockchain el futuro,” *Blockchain: el futuro ya no es lo que era*, 2016. [Online]. Available: https://www.weforum.org/agenda/2016/06/blockchain-explained-

simply/. [Accessed: 07-Sep-2017].

[14] “Qué es blockchain y cómo funciona esta tecnología,” *Whitepaper*, 2017. [Online]. Available: http://www.imnovation.com/es/transformacion-digital/que-es-blockchain-y-como-funciona-esta-tecnologia/. [Accessed: 21-Jul-2017].

[15] M. Antonopoulos, “Mastering Bitcoin,” vol. 2da Edicio, p. 291, 2016.

[16] S. Han, “How does blockchain really work? I built an app to show you.,” 2017. [Online]. Available: https://medium.freecodecamp.org/how-does-blockchain-really-work-i-built-an-app-to-show-you-6b70cd4caf7d. [Accessed: 15-Oct-2017].

[17] J. Guggiari, “BlockChain: La tecnología que descentraliza al mundo.,” p. 6, 2015.

[18] “Bitcoin vs Ethereum,” *MiEthereum. Barcelona-Madrid*, 2018. [Online]. Available: https://miethereum.com/ether/bitcoin-vs-ethereum/#toc1. [Accessed: 05-Feb-2018].

[19] “La tecnología Blockchain en el sistema Bitcoin,” Equipo Fintech, 2017.

[20] “Informe sobre Blockchain,” *Unidad Estud. y Proy. Espec.*, pp. 1–3, 2018.

[21] M. Allende and V. C. Unda, “Blockchain cómo desarrollar confianza en entornos complejos para generar valor de impacto social,” *ITE/IPS TechLab*, p. 49, 2018.

[22] “Join the Ethereum Chile community on Slack!,” *Slack*. [Online]. Available: https://ethereumchile-slack-invite.herokuapp.com/. [Accessed: 13-Mar-2017].

[23] R. Ganghi and A. Ramasastri, “Applications of Blockchain Technology to Banking and Financial Sector in India,” *Inst. Dev. Res. Bankin Technol. IDRBT*, p. 32.

[24] “Las 5 mejores plataformas de blockchain empresarial,” *Serrotho*, 2018. [Online]. Available: http://blog.techdata.com/ts/latam/las-5-mejores-plataformas-de-blockchain. [Accessed: 18-Jan-2018].

[25] “Capitalización de mercado de Criptomoneda,” *CoinMarketCap*, 2018. [Online]. Available: https://coinmarketcap.com/es/. [Accessed: 21-Mar-2018].

[26] “Business in the age of Ethereum,” *TechCrunch*, 2017. [Online]. Available: https://techcrunch.com/2017/06/04/business-in-the-age-of-ethereum/. [Accessed: 14-Jan-2018].

[27] “Ethereum Basic,” *GitHub*, 2018. [Online]. Available: https://github.com/ethereumbook/ethereumbook/blob/develop/intro.asciidoc. [Accessed: 22-Mar-2018].

[28] “Estándares ERC para impulsar el desarrollo de Ethereum ERC-20, ERC-223, ERC-721,” *Logart WePower*, 2017. .

[29] J. Surga, “¿Qué son los Tokens ERC20 de Ethereum y cómo funcionan?,” *CriptoNoticias*, 2017.

[30] Y. Sompolinsky and A. Zohar, “Accelerating Bitcoin’s Transaction Processing. Fast Money Grows on Trees, Not Chains,” *IACR Cryptol. ePrint Arch.*, vol. 881, pp. 1–31, 2013.

[31] E. Ferreño, “Bitcoin vs Ethereum: similitudes y diferencias,” 2017. [Online]. Available: https://www.profesionalreview.com/2017/07/13/bitcoin-vs-ethereum-similitudes-y-diferencias/. [Accessed: 04-Jun-2017].

[32] “Proof of Stake (PoS) o Prueba de Participación en Criptomonedas,” *Mundobitcoin*, 2017. [Online]. Available: https://latinotoken.com/proof-of-stake-pos-prueba-participacion-criptomonedas/. [Accessed: 25-Nov-2017].

[33] “Blockchain Enigma. Paradox. Opportunity,” *Deloitte LLP*, p. 27, 2016.

[34] “Problems at Twitter,” *DownDetector*, 2018. [Online]. Available: http://downdetector.com/status/twitter/news/211816-problems-at-twitter-3. [Accessed: 20-Feb-2018].

[35] “European Commission launches the EU Blockchain Observatory and Forum.” p. 2, 2018.

[36] “Filecoin : A Decentralized Storage Network,” *Protoc. Labs*, pp. 1–36, 2018.

[37] “Lista de los proyectos Blockchain,” *Bitcoin Wiki*, 2018. [Online]. Available: https://es.bitcoinwiki.org/wiki/Lista_de_los_proyectos_Blockchain. [Accessed: 15-Mar-2018].

[38] J. Greenough, “Internet of everything.” BI - Business Insider, 2015.

[39] “Decentralized, anonymous, trustless APIs.” EtherAPIs, 2016.

[40] G. Wood, “Ethereum: a secure decentralised generalised transaction ledger,” *Ethereum Proj. Yellow Pap.*, pp. 1–32, 2014.

[41] J. Tam, G. Vera, and R. Oliveros, “Tipos, métdos y estrategias de Investigación Científica.” pp. 145–154, 2018.

[42] R. Hernández, C. Fernández, P. Baptista, R. Hernandez Sampieri, C. Fernandez

Collado, and M. del P. Baptista Lucio, *Metodología de la Investigación*, McGraw-H. Colombia, 1991.

[43] H. Cerda, “Capítulo 7 : Medios , Instrumentos , Técnicas y Métodos en la Recolección de Datos e Información,” *Bogotá El Buho*, pp. 235–339, 1991.

[44] *Ordenanza N158 Concejo Metropolitano de Quito*. 2011.

[45] “Ministerio del Interior implementa sistema integral de alarmas comunitarias,” 2016. [Online]. Available: https://www.ministeriointerior.gob.ec/ministerio-del-interior-implementa-sistema-integral-de-alarmas-comunitarias/. [Accessed: 27-Jul-2018].

[46] “Planos de casas modernas de 3 pisos,” *Colorlib*, 2015. [Online]. Available: https://planosdecasasmodernas.com/planos-de-casas-modernas-de-3-pisos/. [Accessed: 17-Apr-2017].

[47] “Delitos y violencia del DMQ,” *Munic. del Dist. Metrop. Qutio*, p. 40, 2013.

[48] “¿Cómo puede controlar la seguridad de su casa desde el celular?,” *El Comercio*, 2016. [Online]. Available: https://www.elcomercio.com/actualidad/controlar-seguridad-evitar-robos-casa.html. [Accessed: 16-Jun-2017].

[49] “Integración Sistemas de Seguridad,” *Asociación Latinoamericana de Seguridad*, 2017. [Online]. Available: http://alas-la.org/. [Accessed: 13-Jul-2018].

[50] “Transaction propagation issue on private test net since geth 1.4.6,” *GitHub*, 2016. [Online]. Available: https://github.com/ethereum/go-ethereum/issues/2769#issuecomment-230249342. [Accessed: 15-Mar-2017].

[51] L. Carbonell, “Raspberry Pi,” 2017. [Online]. Available: https://www.atareao.es/tutorial/raspberry-pi-primeros-pasos/. [Accessed: 24-Jun-2017].

[52] “EGPIO,” *Makielectronic*, 2017. [Online]. Available: https://makielectronic.com/detalle.php?productoid=300. [Accessed: 18-Sep-2017].

[53] “Como minar Ethereum en una PC (2018),” *Tecnobits*, 2018. [Online]. Available: http://tecnobits.xyz/como-minar-ethereum-en-una-pc/. [Accessed: 17-Jan-2018].

[54] S. Eloudrhiri, “Set up the private chain-miners,” 2017. [Online]. Available: http://chainskills.com/2017/03/10/part-3-setup-the-private-chain-miners/. [Accessed: 18-Jun-2017].

[55] R. Horrocks, “Ethereum,” 2017. [Online]. Available:

https://ethereum.stackexchange.com/questions/15682/the-meaning-specification-of-config-in-genesis-json. [Accessed: 21-Jul-2017].

[56] D. Egan, “Install and Run Geth (golang implemenation of Ethereum) on Ubuntu,” 2017. [Online]. Available: https://www.dev-notes.eu/2017/07/install-and-run-ethereum-on-ubuntu/l. [Accessed: 27-Aug-2017].

[57] “Command line options,” *GitHub*, 2017. [Online]. Available: https://github.com/ethereum/go-ethereum/wiki/Command-Line-Options. [Accessed: 16-Sep-2017].

[58] “GPIO in Python,” *Raspberry Pi Foundation Uk*, 2017. [Online]. Available: https://www.raspberrypi.org/documentation/usage/gpio/python/README.md. [Accessed: 03-Apr-2017].

[59] C. Metz, “How GitHub conquered Google, Microsoft, and everyone else,” *Wired*, 2015. [Online]. Available: https://www.wired.com/2015/03/github-conquered-google-microsoft-everyone-else/. [Accessed: 16-May-2018].

[60] A. Becerril, “El consorcio de blockchain R3 obtiene 107,” *El Economista*, 2017. [Online]. Available: https://www.eleconomista.com.mx/tecnologia/El-consorcio-de-blockchain-R3-obtiene-107-mdd--20170524-0116.html. [Accessed: 04-Aug-2017].

[61] “Solidity Features,” *GitHub*, 2017. [Online]. Available: https://github.com/ethereum/wiki/wiki/Solidity-Features. [Accessed: 26-Jan-2018].

[62] “The Homestead Release,” *Ethereum Community*, 2016. [Online]. Available: https://ethereum-homestead.readthedocs.io/en/latest/introduction/the-homestead-release.html. [Accessed: 18-Nov-2017].

[63] B. Nuttall, “Gpiozero,” *GitHub*, 2015. [Online]. Available: https://gpiozero.readthedocs.io/en/stable/. [Accessed: 15-May-2017].

6. ANEXOS

ANEXO I Reportes de fallas en los sistemas centralizados

ANEXO II Especificaciones Técnicas de LC100 (Formato digital)

ANEXO III Datasheet D273 (Formato digital)

ANEXO IV Especificaciones Técnicas de PC1832 (Formato digital)

ANEXO V Contenido de Transacciones en Blockchain

ANEXO VI Proforma de los Equipos para el sistema de alarmas

ANEXO VII Desglose del análisis del presupuesto basado en APU

ANEXO VIII Proforma de Costo de monitoreo

ANEXO IX Desglose de costo Puntos para alarma

ANEXO X Desglose de los cálculos totales del sistema de alarmas

ANEXO XI Proforma de los accesorios para implementar el nodo

ANEXO XII Proforma de procesador para el Minero

ANEXO XIII Desglose de Costo de Instalación de Software

ANEXO XIV Desglose de Costo de Implementación

ANEXO XV Pruebas de Transacciones en red P2P *Ethereum*

ANEXO XVI Pruebas para crear el Contrato Inteligente

ANEXO I Reportes de fallas en los sistemas centralizados

Falla técnica de twitter

El Anexo I, fue tomado de *Downdetector*, http://downdetector.com/status/twitter/map/ el 17 de abril de 2017, donde muestra el mapa de las fallas técnicas de Twitter a nivel mundial; Japón, el norte de Europa, España, EEUU y Brazil han sido afectados por la caída de este servicio.

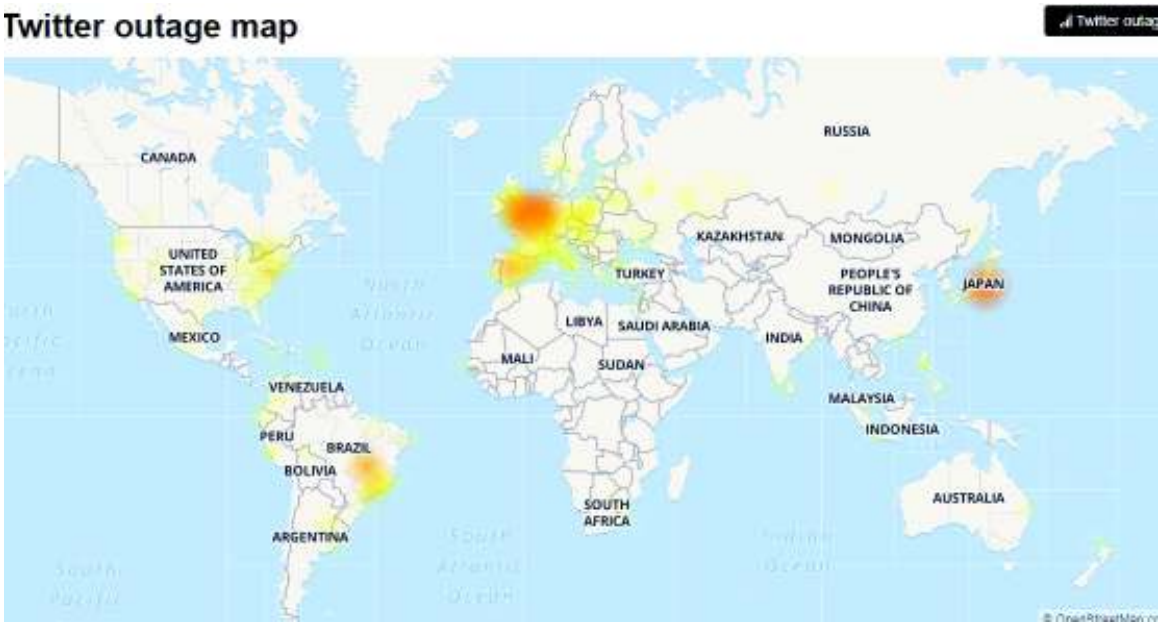

Figura I.1 Mapa de las fallas técnicas de Twitter a nivel mundial [34]

El gráfico estadístico de abajo, indica otra falla técnica que se presentó durante el 26 de mayo a las 14H00 hasta el 27 de mayo a las 13H00. El pico más alto de los problemas en Twitter fue con 609 reportes tanto en la web como en sus aplicaciones móviles.

Figura I.2 Gráfica del reporte de fallo técnico en Twitter [34]

Falla técnica de Facebook

El mapa de fallas técnicas de la red social de Facebook, tomado de la página oficial de *Downdetector* http://downdetector.com/status/facebook/map/, el día 23 de agosto de 2017 a las 11:24, con 382 reportes de fallos.

Figura I.3 Gráfica del reporte de fallo técnico en Facebook 23 de Agosto [34]

En ese mismo mes, el día 26 a las 03H45, vuelve a caer la plataforma, la gráfica de abajo muestra que miles de usuarios se vieron afectados por fallas para acceder a su página.

Figura I.4 Gráfica del reporte de fallo técnico de facebook 26 de Agosto [34]

El 25 de mayo de 2018 desde las 22H20 hasta la tarde del siguiente día, se presentaron fuertes oscilaciones en la red social de Facebook, con el 66% de fallas en el sitio web y el 33% al ingresar al servicio. Los principales inconvenientes se presentaron en España y Chile.

Figura I.5 Gráfica del reporte de fallo técnico de Facebook 25 de Mayo [34]

Fallas técnicas de Movistar

La gráfica de abajo, fue tomada de http://downdetector.com/status/movistar/, indica los problemas que sufrió la red de Movistar el día 22 de marzo de 218, a las 22:12, en países como: Guatemala, Montevideo,

Figura I.6 Gráfica del reporte de fallo técnico en Movistar 22 de Marzo [34]

El 24 de mayo de 2018 desde las 01H29, el servicio de telefonía presento 48 problemas durante varios días irregulares, con varios inconvenientes a nivel mundial

Figura I.7 Gráfica del reporte de fallo técnico en Movistar 24 de Mayo [34]

El mapa de fallas de Telefónica presento problemas del servicio en telefonía móvil, internet, planes de voz y datos en España, Valencia, Granada y Oviedo.

Figura I.8 Mapa de Europa de falla técnica en Movistar [34]

ANEXO II Contenido de Transacciones en *Blockchain*

El Anexo V, fue tomado de https://etherscan.io/txs, el día 29 de Mayo de 2018 a las 22:48. Muestra las 238.101.586 transacciones procesadas, con una altura de 5.700.489 bloques, cuya edad es de 16 segundos, lo que signifique que han transcurrido 16 bloques desde que se registró en la cadena de bloques. Se muestra la dirección origen y destino, el hash de la transacción, entre estos procesos se encuentran encriptados los datos de los usuarios, donde se conserva el anonimato en el proceso.

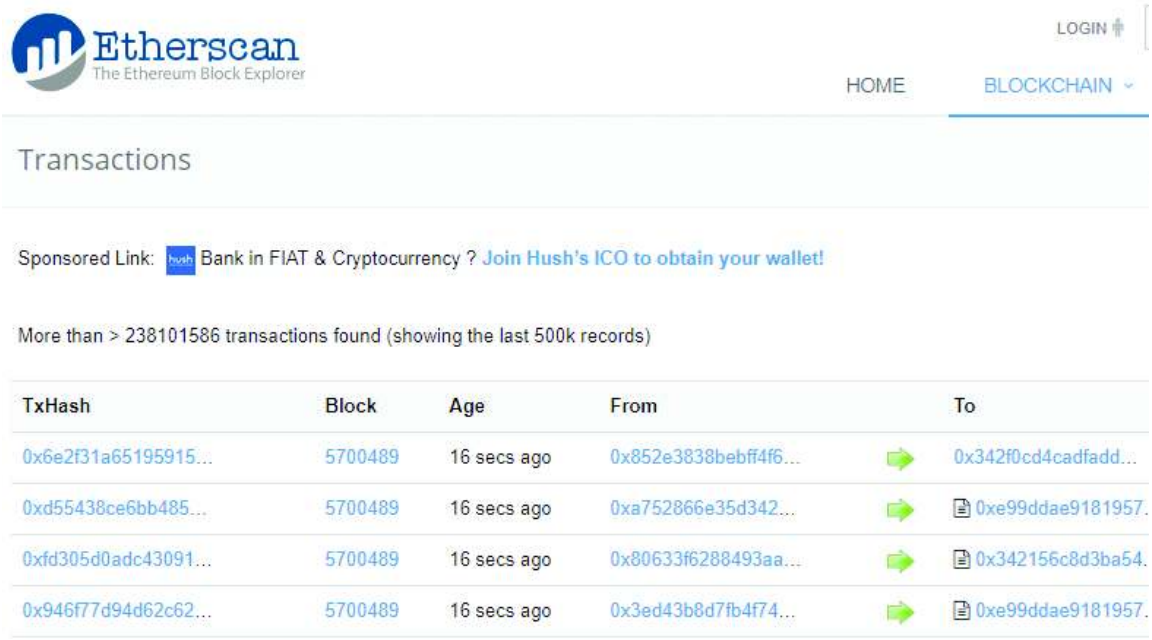

Figura V.1 Transacciones procesadas en Ethereum

Existen 39.606 transacciones pendientes, que se están resolviendo en menos de un minuto. La transacción para que sea procesada necesita de *Gas* que está en Gwei.

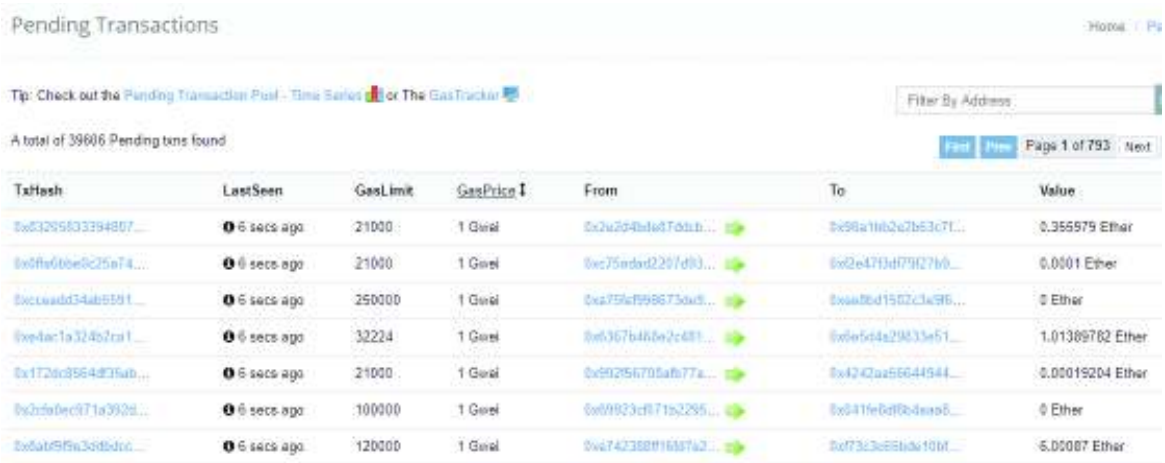

Figura V.2 Transacciones pendientes en Ethereum

El bloque 5.700.489 fue exitosamente procesado en la red, con un proceso de minado de 113 bloques, con un precio de *Gas* de 10Gwei, el valor de procesar el bloque es de 14 centavos. El bloque fue creado el 30 de mayo, con un *Nonce* de valor 1983. La dirección origen y destino, el hash de la transacción, se encuentran encriptados, de esa forma se conserva el anonimato en el sistema.

TxHash:	0x6e2f31a65195915db29ef2b7eab030aac27b5e9d5a723345f109a51ac4fa934e
TxReceipt Status:	Success
Block Height:	5700489 (113 block confirmations)
TimeStamp:	28 mins ago (May-30-2018 03:20:56 AM +UTC)
From:	0x852e3838bebff4f6b1febbec91135dc10c2d19e2
To:	0x342f0cd4cadfadddec18fa116c6d256674214fda
Value:	0.00024 Ether ($0.14)
Gas Limit:	21000
Gas Used By Txn:	21000
Gas Price:	0.00000001 Ether (10 Gwei)
Actual Tx Cost/Fee:	0.00021 Ether ($0.12)
Nonce & {Position}:	1983 | {154}
Input Data:	0x

Figura V.3 Transacciones confirmada en Etherscan

Analizando el figura: Tiempo de procesamiento del Bloque en función del precio, *Gas*. Se concluye que mientras mayor es el precio del *Gas* menor es el tiempo que le toma a la cadena en procesar el bloque.

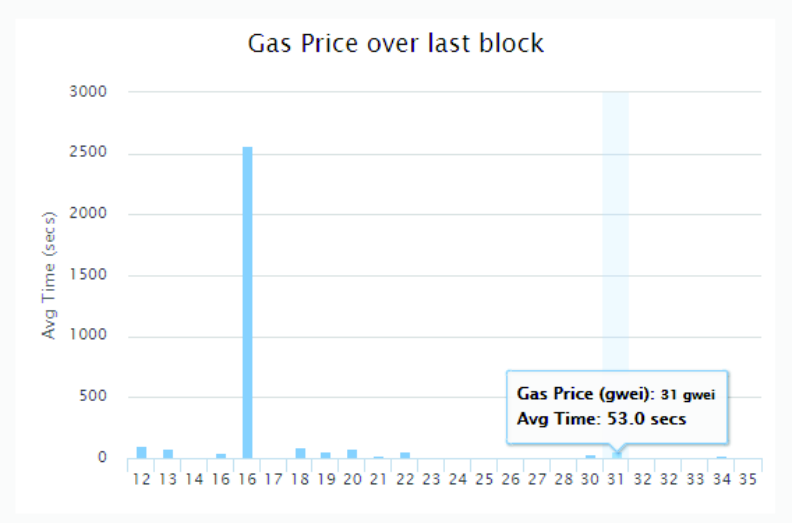

Figura V.4 Precio del gas para procesar el bloque

ANEXO III Proforma de los Equipos para el sistema de alarmas

Proforma No. 02 - 0015264
Fecha Emisión: Marzo 2, 2018
Dias Vigente: 30
Fecha Vencimiento: Abril 1, 2018
ESTADO: VIGENTE

MACROQUIL SA
Sucursal: MATRIZ GUAYAQUIL
Direccion: Urdesa Central Costanera #506 entre Monjas y Ebanos Telf: 2-380484 / 2-885682 -
RUC: 0991382909001

Cliente:
RUC:
Direccion:
Telefono:

Vendedor:

Codigo	Producto	Cantidad	Precio	Total Item
ROK-RK-210PR	DETECTOR MOVIMIENTO COMET PIR 12 METROS	5	$9.01	$45.05
VIP-PH100	DETECTOR DE HUMO PHOTOELECTRICO 4HILOS 12 VOLT N.A	1	$12.94	$12.94
ST-SPB-3045-W	BOTON DE PANICO TIPO PALANCA SENTROL 3045 W	4	$19.31	$77.24
VIP-MC-SFMW	CONTACTO MAGNETICO SOBREPUESTO BLANCO N.C	4	$1.32	$5.28
DSC-PC1832	PANEL ALARMA PC1832 DE 8-32 ZONAS 4 PARTICIONES INCLUYE TECLADO LCD 5511 Y CAJA	1	$107.38	$107.38
MQ-CAJA PANEL ALARMA	CAJA PARA PANELES DE ALARMA MEDIDAS: 24.5 X 27 X 8	1	$0.00	$0.00
DSC-LCD-5511	TECLADO LCD PANELES DSC 1832	1	$50.23	$50.23
VIP-S30	SIRENA DE 30 WATTS DOS TONOS	1	$11.55	$11.55
MQ-CAJA SIREN	CAJA PARA SIRENA	1	$11.63	$11.63

SUBTOTAL:	$321.30
BASE 0%	$0.00
I.V.A. [12.0000%]:	$38.56
ICE [15.00%]:	$0.00
IVA ARRIENDO [12.00%]:	$0.00
TOTAL:	**$359.86**

Son: TRESCIENTOS CINCUENTA Y NUEVE CON 86/100 DOLARES

ANEXO IV Desglose del análisis del presupuesto basado en APU

ANÁLISIS DE PRECIOS UNITARIOS					
NOMBRE DE PROYECTO:	DISEÑO DE ALARMAS CONVENCIONALES EN CASA TIPO				
NOMBRE DE OFERENTE:					
				Hoja 1 de 7	
CÓDIGO RUBRO:	1				
RUBRO:	SENSOR DE MOVIMIENTO			UNIDAD:	U
DETALLE:					
HERRAMIENTA					
DESCRIPCIÓN	CANTIDAD	TARIFA	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Herramienta Menor 5% de M.O. (5% M.O.)					0,07
SUBTOTAL M					0,07
MANO DE OBRA					
DESCRIPCIÓN	CANTIDAD	JORNAL /HR	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Electricista (Estr.Oc D2)	1,00	3,30	3,30	0,2000	0,66
Maestro Electricista (Estr.Oc C1)	1,00	3,66	3,66	0,2000	0,73
SUBTOTAL N					1,39
MATERIALES					
DESCRIPCIÓN		UNIDAD	CANTIDAD	P. UNITARIO	COSTO
			A	B	C = A x B
Detector de Movimiento Antimascotas		u	1,00	9,01	9,01
SUBTOTAL O					9,01
TRANSPORTE					
DESCRIPCIÓN	UNIDAD	DISTANCIA	CANTIDAD	TARIFA	COSTO
			A	B	C = A x B
SUBTOTAL P					0,00
		TOTAL COSTO DIRECTO (M+N+O+P)			10,47
		COSTOS INDIRECTOS		20%	2,09
ESTOS PRECIOS NO INCLUYEN EL IVA		OTROS INDIRECTOS:			
		COSTO TOTAL DEL RUBRO:			12,56
		VALOR OFERTADO:			12,56

ANÁLISIS DE PRECIOS UNITARIOS					
NOMBRE DE PROYECTO:	DISEÑO DE ALARMAS CONVENCIONALES EN CASA TIPO				
NOMBRE DE OFERENTE:					
				Hoja 2 de 7	
CÓDIGO RUBRO:	2				
RUBRO:	DETECTOR DE HuMO			UNIDAD:	U
DETALLE:					

HERRAMIENTA					
DESCRIPCIÓN	CANTIDAD	TARIFA	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Herramienta Menor 5% de M.O. (5% M.O.)					0,07
SUBTOTAL M					0,07
MANO DE OBRA					
DESCRIPCIÓN	CANTIDAD	JORNAL /HR	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Electricista (Estr.Oc D2)	1,00	3,30	3,30	0,2000	0,66
Maestro Electricista (Estr.Oc C1)	1,00	3,66	3,66	0,2000	0,73
SUBTOTAL N					1,39
MATERIALES					
DESCRIPCIÓN		UNIDAD	CANTIDAD	P. UNITARIO	COSTO
			A	B	C = A x B
Detector de Humo Photoeléctrico 12/24 VOLT 4 hilos		U	1,00	12,94	12,94
SUBTOTAL O					12,94
TRANSPORTE					
DESCRIPCIÓN	UNIDAD	DISTANCIA	CANTIDAD	TARIFA	COSTO
			A	B	C = A x B
SUBTOTAL P					0,00

	TOTAL COSTO DIRECTO (M+N+O+P)		14,40
	COSTOS INDIRECTOS	20%	2,88
ESTOS PRECIOS NO INCLUYEN EL IVA	OTROS INDIRECTOS:		
	COSTO TOTAL DEL RUBRO:		17,28
	VALOR OFERTADO:		17,28

ANÁLISIS DE PRECIOS UNITARIOS					
NOMBRE DE PROYECTO:	DISEÑO DE ALARMAS CONVENCIONALES EN CASA TIPO				
NOMBRE DE OFERENTE:					
				Hoja 3 de 7	
CÓDIGO RUBRO:	3				
RUBRO:	BOTÓN DE PÁNICO			UNIDAD:	U
DETALLE:					

EQUIPOS					
DESCRIPCIÓN	CANTIDAD	TARIFA	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Herramienta Menor 5% de M.O. (5% M.O.)					0,07
SUBTOTAL M					0,07
HERRAMIENTA					
DESCRIPCIÓN	CANTIDAD	JORNAL /HR	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Electricista (Estr.Oc D2)	1,00	3,30	3,30	0,2000	0,66
Maestro Electricista (Estr.Oc C1)	1,00	3,66	3,66	0,2000	0,73
SUBTOTAL N					1,39
MATERIALES					
DESCRIPCIÓN		UNIDAD	CANTIDAD	P. UNITARIO	COSTO
			A	B	C = A x B
Botón de Pánico Doméstico		u	1,00	19,31	19,31
SUBTOTAL O					19,31
TRANSPORTE					
DESCRIPCIÓN	UNIDAD	DISTANCIA	CANTIDAD	TARIFA	COSTO
			A	B	C = A x B
SUBTOTAL P					0,00
		TOTAL COSTO DIRECTO (M+N+O+P)			20,77
		COSTOS INDIRECTOS		20%	4,15
ESTOS PRECIOS NO INCLUYEN EL IVA		OTROS INDIRECTOS:			
		COSTO TOTAL DEL RUBRO:			24,92
		VALOR OFERTADO:			24,92

ANÁLISIS DE PRECIOS UNITARIOS					
NOMBRE DE PROYECTO:	DISEÑO DE ALARMAS CONVENCIONALES EN CASA TIPO				
NOMBRE DE OFERENTE:					
				Hoja 4 de 7	
CÓDIGO RUBRO:	4				
RUBRO:	CONTACTO MAGNÉTICO			UNIDAD:	U
DETALLE:					

HERRAMIENTA					
DESCRIPCIÓN	CANTIDAD	TARIFA	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Herramienta Menor 5% de M.O. (5% M.O.)					0,04
SUBTOTAL M					0,04
MANO DE OBRA					
DESCRIPCIÓN	CANTIDAD	JORNAL /HR	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Electricista (Estr.Oc D2)	1,00	3,30	3,30	0,1000	0,33
Maestro Electricista (Estr.Oc C1)	1,00	3,66	3,66	0,1000	0,37
SUBTOTAL N					0,70
MATERIALES					
DESCRIPCIÓN		UNIDAD	CANTIDAD	P. UNITARIO	COSTO
			A	B	C = A x B
Contacto Magnético		U	1,00	1,32	1,32
SUBTOTAL O					1,32
TRANSPORTE					
DESCRIPCIÓN	UNIDAD	DISTANCIA	CANTIDAD	TARIFA	COSTO
			A	B	C = A x B
SUBTOTAL P					0,00
		TOTAL COSTO DIRECTO (M+N+O+P)			2,06
		COSTOS INDIRECTOS		20%	0,41
ESTOS PRECIOS NO INCLUYEN EL IVA		OTROS INDIRECTOS:			
		COSTO TOTAL DEL RUBRO:			2,47
		VALOR OFERTADO:			2,47

ANÁLISIS DE PRECIOS UNITARIOS					
NOMBRE DE PROYECTO:	DISEÑO DE ALARMAS CONVENCIONALES EN CASA TIPO				
NOMBRE DE OFERENTE:					
				Hoja 5 de 7	
CÓDIGO RUBRO:	5				
RUBRO:	TECLADO DE CONTROL			UNIDAD:	U
DETALLE:					

HERRAMIENTA					
DESCRIPCIÓN	CANTIDAD	TARIFA	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Herramienta Menor 5% de M.O. (5% M.O.)					0,13
SUBTOTAL M					0,13
MANO DE OBRA					
DESCRIPCIÓN	CANTIDAD	JORNAL /HR	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Peón de Electricista (Estr.Oc E2)	1,00	3,26	3,26	0,4000	1,30
Electricista (Estr.Oc D2)	1,00	3,30	3,30	0,4000	1,32
SUBTOTAL N					2,62
MATERIALES					
DESCRIPCIÓN		UNIDAD	CANTIDAD	P. UNITARIO	COSTO
			A	B	C = A x B
Teclado LCD Paneles DSC 1832		U	1,00	50,23	50,23
SUBTOTAL O					50,23
TRANSPORTE					
DESCRIPCIÓN	UNIDAD	DISTANCIA	CANTIDAD	TARIFA	COSTO
			A	B	C = A x B
SUBTOTAL P					0,00
		TOTAL COSTO DIRECTO (M+N+O+P)			52,98
		COSTOS INDIRECTOS		20%	10,60
ESTOS PRECIOS NO INCLUYEN EL IVA		OTROS INDIRECTOS:			
		COSTO TOTAL DEL RUBRO:			63,58
		VALOR OFERTADO:			63,58

ANÁLISIS DE PRECIOS UNITARIOS					
NOMBRE DE PROYECTO:	DISEÑO DE ALARMAS CONVENCIONALES EN CASA TIPO				
NOMBRE DE OFERENTE:					
				Hoja 6 de 7	
CÓDIGO RUBRO:	6				
RUBRO:	PANEL DE ALARMAS INCLuYE TECLADO Y CAJA			UNIDAD:	U
DETALLE:					

HERRAMIENTA					
DESCRIPCIÓN	CANTIDAD	TARIFA	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Herramienta Menor 5% de M.O. (5% M.O.)					0,96
SUBTOTAL M					0,96
MANO DE OBRA					
DESCRIPCIÓN	CANTIDAD	JORNAL /HR	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Electricista (Estr.Oc D2)	1,00	3,30	3,30	1,0000	3,30
Maestro Electricista (Estr.Oc C1)	1,00	3,66	3,66	1,0000	3,66
Ingeniero Electrónico Especializado	1,00	12,30	12,30	1,0000	12,30
SUBTOTAL N					19,26
MATERIALES					
DESCRIPCIÓN		UNIDAD	CANTIDAD	P. UNITARIO	COSTO
			A	B	C = A x B
Panel de alarma PC1832 de 8-32 Zonas de 4 Particiones Incluye Teclado LCD 5511 y Caja		U	1,00	107,38	107,38
SUBTOTAL O					107,38
TRANSPORTE					
DESCRIPCIÓN	UNIDAD	DISTANCIA	CANTIDAD	TARIFA	COSTO
			A	B	C = A x B
SUBTOTAL P					0,00

	TOTAL COSTO DIRECTO (M+N+O+P)		127,60
	COSTOS INDIRECTOS	20%	25,52
ESTOS PRECIOS NO INCLUYEN EL IVA	OTROS INDIRECTOS:		
	COSTO TOTAL DEL RUBRO:		153,12
	VALOR OFERTADO:		153,12

ANÁLISIS DE PRECIOS UNITARIOS					
NOMBRE DE PROYECTO:	DISEÑO DE ALARMAS CONVENCIONALES EN CASA TIPO				
NOMBRE DE OFERENTE:					
				Hoja 7 de 7	
CÓDIGO RUBRO:	7				
RUBRO:	SIRENA EXTERIOR			UNIDAD:	U
DETALLE:					

HERRAMIENTA					
DESCRIPCIÓN	CANTIDAD	TARIFA	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Herramienta Menor 5% de M.O. (5% M.O.)					0,17
SUBTOTAL M					0,17

MANO DE OBRA					
DESCRIPCIÓN	CANTIDAD	JORNAL /HR	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Electricista (Estr.Oc D2)	1,00	3,30	3,30	0,5000	1,65
Maestro Electricista (Estr.Oc C1)	1,00	3,66	3,66	0,5000	1,83
SUBTOTAL N					3,48

MATERIALES				
DESCRIPCIÓN	UNIDAD	CANTIDAD	P. UNITARIO	COSTO
		A	B	C = A x B
Sirena 30 WATT	U	1,00	11,55	11,55
Caja para Sirena	U	1,00	11,63	11,63
SUBTOTAL O				23,18

TRANSPORTE					
DESCRIPCIÓN	UNIDAD	DISTANCIA	CANTIDAD	TARIFA	COSTO
			A	B	C = A x B
SUBTOTAL P					0,00

	TOTAL COSTO DIRECTO (M+N+O+P)		26,83
	COSTOS INDIRECTOS	20%	5,37
ESTOS PRECIOS NO INCLUYEN EL IVA	OTROS INDIRECTOS:		
	COSTO TOTAL DEL RUBRO:		32,20
	VALOR OFERTADO:		32,20

ANEXO V Proforma de Costo de monitoreo

CGB

MONITOREO DE ALARMAS CGB

(ENERO/2017)

DESCRIPCIÓN DE NUESTROS SERVICIOS	Monitoreo Electrónico	Monitoreo Electrónico con VFE	Monitoreo Interactivo****	Monitoreo Interactivo con VFE****
Supervisión de conexiones y desconexiones del sistema de alarma con identificación individual de cada usuario a través de nuestra estación central de monitoreo 24/7.	✓	✓	✓	✓
Aplicación de protocolos de seguridad diseñados para el cliente ante eventos de emergencia por señales emitidas por el sistema de alarma, estos incluyen llamada inmediata a los organismos pertinentes (Policía Nacional - UPC más cercano, Bomberos, guardias privados asignados por el cliente).	✓	✓	✓	✓
Llamada de verificación en eventos de emergencia a los teléfonos provistos por el cliente.	✓	✓	✓	✓
Recepción de eventos de alarma y restauración con identificación de zonas.	✓	✓	✓	✓
Pruebas periódicas de comunicación para garantizar la comunicación de su panel con nuestra Estación Central 24/7.	✓	✓	✓	✓
Monitoreo permanente de las señales enviadas por el sistema para un adecuado mantenimiento preventivo.	✓	✓	✓	✓
Envío de eventos de conexión, desconexión, alarma y cortes de energía eléctrica por e-mail o SMS.	✓	✓	✓	✓
Control de horarios de conexión y desconexión del sistema de alarma.**	✓	✓	✓	✓
Visitas técnicas sin costo dentro del área urbana de la Ciudad de Quito. Esto no incluye el cambio o adición de componentes al sistema de alarma por daño o a solicitud del cliente.	✓	✓	✓	✓
Verificación física de emergencias en las instalaciones monitoreadas con personal debidamente capacitado y equipado.*		✓		✓
Monitoreo Electrónico 3G del sistema de alarma 24 horas al día (3G: monitoreo de su sistema de alarma a través de la red de datos celular-GPRS).			✓	✓
Aplicación web y móvil(a través de su celular) para conectar o desconectar el panel de alarma remotamente.			✓	✓
Recepción de notificaciones de alarmas, conexiones, desconexiones y reportes de estatus a través de aplicación móvil.			✓	✓
Notificaciones 24/7 a través de la aplicación móvil o via e-mail, del cambio de estado de hasta 10 zonas o sensores de su sistema de seguridad. Esto es independiente de que el sistema esta activado o desactivado.			✓	✓
Automatización: control de luces, cerraduras, termostatos y cualquier dispositivo compatible con sistemas Z-Wave.			✓	✓

FORMAS DE PAGO				
Débito mensual a través de su tarjeta de crédito Diners Club, Visa o Mastercard, o a través de un débito bancario de cualquier institución financiera registrada en el Banco Central del Ecuador. Valor de su pago mensual (no incluye IVA):	$ 20,00	$ 29,50	$ 25,00	$ 35,00
8% de descuento si su pago lo hace de manera semestral por anticipado (no incluye IVA)***:	$ 110,40	$ 162,84	$ 138,00	$ 193,20

OBSERVACIONES

- * SERVICIO SUJETO A VERIFICACION DE COBERTURA POR PARTE DE LAS PATRULLAS DE CGB.
- ** SERVICIO DISPONIBLE EXCLUSIVAMENTE PARA EMPRESAS.
- *** EL VALOR DE DESCUENTO SE OTORGA SOLO EN PAGOS CON EFECTIVO O CHEQUE.
- **** EL SERVICIO INTERACTIVO REQUIERE PANELES NEO O IMPASSA, CONSULTE CON SU ASESOR SOBRE NUESTRAS PROMOCIONES.

ANEXO VI Desglose de costo Puntos para alarma

ANÁLISIS DE PRECIOS UNITARIOS					
NOMBRE DE PROYECTO:	DISEÑO DE ALARMAS CONVENCIONALES EN CASA TIPO				
NOMBRE DE OFERENTE:					
				Hoja 1 de 5	
CÓDIGO RUBRO:	1				
RUBRO:	PUNTO PARA ALARMA TIPO A			UNIDAD:	PUNTO
DETALLE:					
HERRAMIENTA					
DESCRIPCIÓN	CANTIDAD	TARIFA	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Herramienta Menor 5% de M.O. (5% M.O.)					0,21
SUBTOTAL M					0,21
MANO DE OBRA					
DESCRIPCIÓN	CANTIDAD	JORNAL /HR	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Electricista (Estr.Oc D2)	1,00	3,30	3,30	0,6000	1,98
Maestro Electricista (Estr.Oc C1)	1,00	3,66	3,66	0,6000	2,20
SUBTOTAL N					4,18
MATERIALES					
DESCRIPCIÓN		UNIDAD	CANTIDAD	P. UNITARIO	COSTO
			A	B	C = A x B
Caja Rectangular		U	1,00	0,35	0,35
Material Menudo		GLB	0,10	11,30	1,13
Abrazadera EMT 1/2"		U	3,00	0,03	0,09
Conector Conduit EMT de 1/2"		UND	4,00	0,25	1,00
Cable UTP 5E		M	7,00	0,45	3,15
Cable Gemelo 2x16		M	7,00	0,21	1,47
Tuberia Conduit EMT 1/2"		M	6,00	1,02	6,12
SUBTOTAL O					13,31
TRANSPORTE					
DESCRIPCIÓN	UNIDAD	DISTANCIA	CANTIDAD	TARIFA	COSTO
			A	B	C = A x B
SUBTOTAL P					0,00
		TOTAL COSTO DIRECTO (M+N+O+P)			17,70
		COSTOS INDIRECTOS		20%	3,54
ESTOS PRECIOS NO INCLUYEN EL IVA		OTROS INDIRECTOS:			
		COSTO TOTAL DEL RUBRO:			21,24
		VALOR OFERTADO:			21,24

ANÁLISIS DE PRECIOS UNITARIOS					
NOMBRE DE PROYECTO:	DISEÑO DE ALARMAS CONVENCIONALES EN CASA TIPO				
NOMBRE DE OFERENTE:					
				Hoja 2 de 5	
CÓDIGO RUBRO:	2				
RUBRO:	PUNTO PARA ALARMA TIPO B			UNIDAD:	PUNTO
DETALLE:					

HERRAMIENTA					
DESCRIPCIÓN	CANTIDAD	TARIFA	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Herramienta Menor 5% de M.O. (5% M.O.)					0,21
SUBTOTAL M					0,21
MANO DE OBRA					
DESCRIPCIÓN	CANTIDAD	JORNAL /HR	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Electricista (Estr.Oc D2)	1,00	3,30	3,30	0,6000	1,98
Maestro Electricista (Estr.Oc C1)	1,00	3,66	3,66	0,6000	2,20
SUBTOTAL N					4,18
MATERIALES					
DESCRIPCIÓN		UNIDAD	CANTIDAD	P. UNITARIO	COSTO
			A	B	C = A x B
Caja Rectangular		U	1,00	0,35	0,35
Material Menudo		GLB	0,10	11,30	1,13
Abrazadera EMT 1/2"		U	3,00	0,03	0,09
Conector Conduit EMT de 1/2"		UND	4,00	0,25	1,00
Cable UTP 5E		M	7,00	0,45	3,15
Tuberia Conduit EMT 1/2"		M	6,00	1,02	6,12
SUBTOTAL O					11,84
TRANSPORTE					
DESCRIPCIÓN	UNIDAD	DISTANCIA	CANTIDAD	TARIFA	COSTO
			A	B	C = A x B
SUBTOTAL P					0,00
		TOTAL COSTO DIRECTO (M+N+O+P)			16,23
		COSTOS INDIRECTOS		20%	3,25
ESTOS PRECIOS NO INCLUYEN EL IVA		OTROS INDIRECTOS:			
		COSTO TOTAL DEL RUBRO:			19,48
		VALOR OFERTADO:			19,48

ANÁLISIS DE PRECIOS UNITARIOS					
NOMBRE DE PROYECTO:	DISEÑO DE ALARMAS CONVENCIONALES EN CASA TIPO				
NOMBRE DE OFERENTE:					
				Hoja 3 de 5	
CÓDIGO RUBRO:	3				
RUBRO:	PUNTO PARA PANEL DE ALARMAS			UNIDAD:	PUNTO
DETALLE:					

HERRAMIENTA					
DESCRIPCIÓN	CANTIDAD	TARIFA	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Herramienta Menor 5% de M.O. (5% M.O.)					0,35
SUBTOTAL M					0,35
MANO DE OBRA					
DESCRIPCIÓN	CANTIDAD	JORNAL /HR	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Electricista (Estr.Oc D2)	1,00	3,30	3,30	1,0000	3,30
Maestro Electricista (Estr.Oc C1)	1,00	3,66	3,66	1,0000	3,66
SUBTOTAL N					6,96
MATERIALES					
DESCRIPCIÓN		UNIDAD	CANTIDAD	P. UNITARIO	COSTO
			A	B	C = A x B
Conector EMT 1/2"		U	2,00	0,38	0,76
Tuberia Conduit EMT 1/2"		M	12,00	1,24	14,88
Unión EMT 1/2 "		U	4,00	0,28	1,12
Caja Rectangular		U	2,00	0,35	0,70
Caja octogonal		U	0,60	0,42	0,25
Caja cuadrada 10X10		U	0,60	1,57	0,94
Cable THHN 12 AWG		M	19,00	0,58	11,02
Material Menudo		GLB	0,02	4,00	0,08
Cable telefónico entorchado AWG 2x17		M	15,00	0,17	2,55
SUBTOTAL O					32,30
TRANSPORTE					
DESCRIPCIÓN	UNIDAD	DISTANCIA	CANTIDAD	TARIFA	COSTO
			A	B	C = A x B
SUBTOTAL P					0,00
		TOTAL COSTO DIRECTO (M+N+O+P)			39,61
		COSTOS INDIRECTOS		20%	7,92
ESTOS PRECIOS NO INCLUYEN EL IVA		OTROS INDIRECTOS:			
		COSTO TOTAL DEL RUBRO:			47,53
		VALOR OFERTADO:			47,53

ANÁLISIS DE PRECIOS UNITARIOS					
NOMBRE DE PROYECTO:	DISEÑO DE ALARMAS CONVENCIONALES EN CASA TIPO				
NOMBRE DE OFERENTE:					
				Hoja 4 de 5	
CÓDIGO RUBRO:	4				
RUBRO:	PUNTO PARA TECLADO			UNIDAD:	PUNTO
DETALLE:					
HERRAMIENTA					
DESCRIPCIÓN	CANTIDAD	TARIFA	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Herramienta Menor 5% de M.O. (5% M.O.)					0,21
SUBTOTAL M					0,21
MANO DE OBRA					
DESCRIPCIÓN	CANTIDAD	JORNAL /HR	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Electricista (Estr.Oc D2)	1,00	3,30	3,30	0,6000	1,98
Maestro Electricista (Estr.Oc C1)	1,00	3,66	3,66	0,6000	2,20
SUBTOTAL N					4,18
MATERIALES					
DESCRIPCIÓN		UNIDAD	CANTIDAD	P. UNITARIO	COSTO
			A	B	C = A x B
Caja Rectangular		u	1,00	0,35	0,35
Material Menudo		GLB	0,10	11,30	1,13
Abrazadera EMT 1/2"		u	3,00	0,03	0,09
Conector Conduit EMT de 1/2"		UND	4,00	0,25	1,00
Cable UTP 5E		M	7,00	0,45	3,15
Tuberia Conduit EMT 1/2"		m	6,00	1,02	6,12
SUBTOTAL O					11,84
TRANSPORTE					
DESCRIPCIÓN	UNIDAD	DISTANCIA	CANTIDAD	TARIFA	COSTO
			A	B	C = A x B
SUBTOTAL P					0,00
		TOTAL COSTO DIRECTO (M+N+O+P)			16,23
		COSTOS INDIRECTOS		20%	3,25
ESTOS PRECIOS NO INCLUYEN EL IVA		OTROS INDIRECTOS:			
		COSTO TOTAL DEL RUBRO:			19,48
		VALOR OFERTADO:			19,48

ANÁLISIS DE PRECIOS UNITARIOS					
NOMBRE DE PROYECTO:	DISEÑO DE ALARMAS CONVENCIONALES EN CASA TIPO				
NOMBRE DE OFERENTE:					
				Hoja 5 de 5	
CÓDIGO RUBRO:	5				
RUBRO:	PUNTO PARA SIRENA			UNIDAD:	PUNTO
DETALLE:					

HERRAMIENTA					
DESCRIPCIÓN	CANTIDAD	TARIFA	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Herramienta Menor 5% de M.O. (5% M.O.)					0,21
SUBTOTAL M					0,21
MANO DE OBRA					
DESCRIPCIÓN	CANTIDAD	JORNAL /HR	COSTO HORA	RENDIMIENTO	COSTO
	A	B	C = A x B	R	D = C x R
Electricista (Estr.Oc D2)	1,00	3,30	3,30	0,6000	1,98
Maestro Electricista (Estr.Oc C1)	1,00	3,66	3,66	0,6000	2,20
SUBTOTAL N					4,18
MATERIALES					
DESCRIPCIÓN		UNIDAD	CANTIDAD	P. UNITARIO	COSTO
			A	B	C = A x B
Caja Rectangular		u	1,00	0,35	0,35
Material Menudo		GLB	0,10	11,30	1,13
Abrazadera EMT 1/2"		u	3,00	0,03	0,09
Conector Conduit EMT de 1/2"		UND	4,00	0,25	1,00
Cable Gemelo 2x16		m	7,00	0,21	1,47
Tuberia Conduit EMT 1/2"		m	6,00	1,02	6,12
SUBTOTAL O					10,16
TRANSPORTE					
DESCRIPCIÓN	UNIDAD	DISTANCIA	CANTIDAD	TARIFA	COSTO
			A	B	C = A x B
SUBTOTAL P					0,00
		TOTAL COSTO DIRECTO (M+N+O+P)			14,55
		COSTOS INDIRECTOS		20%	2,91
ESTOS PRECIOS NO INCLUYEN EL IVA		OTROS INDIRECTOS:			
		COSTO TOTAL DEL RUBRO:			17,46
		VALOR OFERTADO:			17,46

ANEXO VII Desglose de los cálculos totales del sistema de alarmas

PROYECTO: DISEÑO DE ALARMAS CONVENCIONALES EN CASA TIPO

TABLA DE CANTIDADES Y PRECIOS

COD	TIPO DE COSTO	COSTO MENSUAL	COSTO ANUAL
1	EQUIPAMIENTO	438.54	438.54
2	MONITOREO	27.50	330.00
3	INSTALACIÓN	387.23	387.23
4	MANTENIMIENTO	0.00	0.00
	TOTAL	853.27	1,155.77

MIL CIENTO CINCUENTA Y CINCO dólares SETENTA Y SIETE centavos.

NOTA: no incluye IVA vigente

COSTO TOTAL		
30 CASAS	25598.10	**34673.10**

TREINTA Y CUATRO MIL SEIS CIENTOS SETENTA Y TRES DÓLARES CON DIEZ CENTAVO

NOTA: no incluye IVA vigente

ANEXO VIII Proforma de los accesorios para implementar el nodo

ALL POWER MICROCONTROLLER APM
AV. COLON OE3-31 Y VERSALLES LOCAL N°1
1714061932001
022502124

PROFORMA NO.0000007132

CLIENTE:
DIRECCION:
RUC/CI:
FECHA: 02/03/2018 12:34:39 PM

CODIGO	DESCRIPCION	CANT	P.UNIT.	TOTAL
5352	FUENTE RASPBERRY	1.000	11.1607	11.16
6597	RASPBERRY PI 3	1.000	58.0357	58.04
6156	DISIPADOR DE CALOR PARA RASPBERRY X3	1.000	10.7143	10.71
2817	VENT. 1.5" 12V 0.10A	1.000	4.4643	4.46
5828	MICROSD 16G	1.000	16.0000	16.00
6988	PANTALLA 7" NEXTION	1.000	94.6429	94.64
5750	LCD TFT 3.2" MIKROE	1.000	33.0357	33.04

ANEXO IX Proforma de procesador para el Minero

Fech-Impresión 02/mar/2018
Hora-Emisión 12:50:12

PEDIDO No. PED18008871S2

Cliente:
Ruc:
Dirección:
Zona:
Teléfonos: Fax:

Fecha Pedido: 02/mar/2018 12:53:52
Vendedor: 9 - LOURDES MERA
Estatus: ACTIVO
Forma de Pago: EFECTIVO DOLAR

Código	Descripción del Artículo	Cantidad	Valor Unitario	Valor
COPQONMH110I3W1	COP. Q-ONE CORE I3-7100 4GB 1TB VD-SN-RD DW CR	1.00	419.99	419.99

Información del envío:

Subtotal :	419.99
Descuento :	0.00
Base Imponible :	419.99
I.V.A :	50.40
Total :	470.39

Observación:
PROF.

PROFORMA

Elaborado por: Lourdes
Aprobado por: Lourdes

ANEXO X Desglose de Costo de Instalación de Software

TABLA DE VALORES						
NOMBRE DE PROYECTO:	DISEÑO DE ALARMAS CON TECNOLOGÍA BLOCKCHAIN EN CASA TIPO					
NOMBRE DE OFERENTE:						
					Hoja 1 de 2	
CODIGO RUBRO:	1					
RUBRO:	INSTALACIÓN DEL NODO EN RASPEBERRY PI 3					
DETALLE:						
RECURSO HUMANO PARA CONFIGURAR EL SOFTWARE						
DESCRIPCIÓN	RECURSO HUMANO	CANTIDAD	JORNAL /HR	COSTO HORA	RENDIMIENTO	COSTO
		A	B	C = A x B	R	D = C x R
Instalación del Raspbian en RPI	Técnico Instalador (Estr.Oc C1)	1,00	3,74	3,74	1,0000	3,74
Instalación de Geth 1.8.1 en RPI	Ingeniero en Sistemas	1,00	4,58	4,58	0,6000	2,75
SUBTOTAL M						2,75
			TOTAL COSTO DIRECTO (M)			2,75
			COSTOS INDIRECTOS		20%	0,55
ESTOS PRECIOS NO INCLUYEN EL IVA			OTROS INDIRECTOS:			
			COSTO TOTAL DEL RUBRO:			3,30
			VALOR OFERTADO:			3,30

TABLA DE VALORES						
NOMBRE DE PROYECTO:	DISEÑO DE ALARMAS CON TECNOLOGÍA BLOCKCHAIN EN CASA TIPO					
NOMBRE DE OFERENTE:						
					Hoja 2 de 2	
CODIGO RUBRO:	2					
RUBRO:	INSTALACIÓN DEL NODO EN RASPEBERRY PI 3					
DETALLE:						
RECURSO HUMANO PARA CONFIGURAR EL SOFTWARE						
DESCRIPCIÓN	RECURSO HUMANO	CANTIDAD	JORNAL /HR	COSTO HORA	RENDIMIENTO	COSTO
		A	B	C = A x B	R	D = C x R
Instalación de Ubuntu 16.04 en la PC	Técnico Instalador (Estr.Oc C1)	1,00	3,74	3,74	1,0000	3,74
Instalación de Geth 1.8.6 en la PC	Ingeniero en Sistemas	1,00	4,58	4,58	1,5000	6,87
SUBTOTAL M						10,61
			TOTAL COSTO DIRECTO (M)			10,61
			COSTOS INDIRECTOS		20%	2,12
ESTOS PRECIOS NO INCLUYEN EL IVA			OTROS INDIRECTOS:			
			COSTO TOTAL DEL RUBRO:			12,73
			VALOR OFERTADO:			12,73

PROYECTO: DISEÑO DE ALARMAS CON TECNOLOGÍA BLOCKCHAIN EN CASA TIPO

TABLA DE CANTIDADES Y PRECIOS

COD	DESCRIPCIÓN	UNIDAD	P/H	TOTAL
1	INSTALACIÓN DEL NODO EN EL RASPBERRY	30,00	3,30	99,00
2	INSTALACIÓN DEL MINERO EN LA PC	4,00	12,73	50,92
		TOTAL:		149,92

ANEXO XI Desglose de Costo de Implementación

TABLA DE VALORES						
NOMBRE DE PROYECTO:	DISEÑO DE ALARMAS CON TECNOLOGIA BLOCKCHAIN EN CASA TIPO					
NOMBRE DE OFERENTE:						
					Hoja 1 de 3	
CÓDIGO RUBRO:	1					
RUBRO:	IMPLEMENTACIÓN DEL NODO EN RASPEBERRY PI 3					
DETALLE:						
RECURSO HUMANO PARA CONFIGURAR EL SOFTWARE						
DESCRIPCIÓN	RECURSO HUMANO	CANTIDAD	JORNAL /HR	COSTO HORA	RENDIMIENTO	COSTO
		A	B	C = A x B	R	D = C x R
Configuración del nodo RPI	Ingeniero en Sistemas	1,00	4,58	4,58	1,0000	4,58
Recepción de los eventos desde el panel al RPI	Ingeniero en Sistemas	1,00	4,58	4,58	2,0000	9,16
Sincronización del nodo con el minero	Ingeniero en Sistemas	1,00	4,58	4,58	1,5000	6,87
Notificación de los eventos a los nodos de red P2P	Ingeniero en Sistemas	1,00	4,58	4,58	1,0000	4,58
SUBTOTAL M						25,19
			TOTAL COSTO DIRECTO (M)			25,19
			COSTOS INDIRECTOS		20%	5,04
ESTOS PRECIOS NO INCLUYEN EL IVA			OTROS INDIRECTOS:			
			COSTO TOTAL DEL RUBRO:			30,23
			VALOR OFERTADO:			30,23

TABLA DE VALORES						
NOMBRE DE PROYECTO:	DISEÑO DE ALARMAS CON TECNOLOGIA BLOCKCHAIN EN CASA TIPO					
NOMBRE DE OFERENTE:						
					Hoja 2 de 3	
CÓDIGO RUBRO:	2					
RUBRO:	IMPLEMENTACIÓN DEL NODO EN RASPEBERRY PI 3					
DETALLE:						
RECURSO HUMANO PARA CONFIGURAR EL SOFTWARE						
DESCRIPCIÓN	RECURSO HUMANO	CANTIDAD	JORNAL /HR	COSTO HORA	RENDIMIENTO	COSTO
		A	B	C = A x B	R	D = C x R
Configuración del minero en la PC	Ingeniero en Sistemas	1,00	4,58	4,58	2,0000	9,16
Sincronización entre los mineros	Ingeniero en Sistemas	1,00	4,58	4,58	2,5000	11,45
SUBTOTAL M						20,61
			TOTAL COSTO DIRECTO (M)			20,61
			COSTOS INDIRECTOS		20%	4,12
ESTOS PRECIOS NO INCLUYEN EL IVA			OTROS INDIRECTOS:			
			COSTO TOTAL DEL RUBRO:			24,73
			VALOR OFERTADO:			24,73

TABLA DE VALORES						
NOMBRE DE PROYECTO:	DISEÑO DE ALARMAS CON TECNOLOGIA BLOCKCHAIN EN CASA TIPO					
NOMBRE DE OFERENTE:						
					Hoja 3 de 3	
CÓDIGO RUBRO:	3					
RUBRO:	IMPLEMENTACIÓN DEL CONTRATO INTELIGENTE					
DETALLE:						
RECURSO HUMANO PARA CONFIGURAR EL SOFTWARE						
DESCRIPCIÓN	RECURSO HUMANO	CANTIDAD	JORNAL /HR	COSTO HORA	RENDIMIENTO	COSTO
		A	B	C = A x B	R	D = C x R
Desarrollo del Contrato Inteligente	Ingeniero en Sistemas	1,00	4,58	4,58	2,0000	9,16
Sincronización con nodos de red P2P	Ingeniero en Sistemas	1,00	4,58	4,58	3,0000	13,74
SUBTOTAL M						22,90
			TOTAL COSTO DIRECTO (M)			22,90
			COSTOS INDIRECTOS		20%	4,58
ESTOS PRECIOS NO INCLUYEN EL IVA			OTROS INDIRECTOS:			
			COSTO TOTAL DEL RUBRO:			27,48
			VALOR OFERTADO:			27,48

PROYECTO: DISEÑO DE ALARMAS CON TECNOLOGIA BLOCKCHAIN EN CASA TIPO

TABLA DE CANTIDADES Y PRECIOS

COD	DESCRIPCIÓN	CANT	P.UNITARIO	TOTAL
1	IMPLEMENTACIÓN DEL NODO EN EL RASPBERRY	30,00	30,23	906,90
2	IMPLEMENTACIÓN DEL MINERO EN LA PC	4,00	24,73	98,92
3	IMPLEMENTACIÓN DEL CONTRATO INTELIGENTE	1,00	27,48	27,48
		TOTAL:		1.033,30

TABLA DE VALORES						
NOMBRE DE PROYECTO:	DISEÑO DE ALARMAS CON TECNOLOGÍA BLOCKCHAIN EN CASA TIPO					
NOMBRE DE OFERENTE:						
					Hoja 1 de 1	
CÓDIGO RUBRO:	1					
RUBRO:	MANTENIMIENTO DE RED P2P					
DETALLE:						
RECURSO HUMANO PARA CONFIGURAR EL SOFTWARE						
DESCRIPCIÓN	RECURSO HUMANO	CANTIDAD	JORNAL /HR	COSTO HORA	RENDIMIENTO	COSTO
		A	B	C = A x B	R	D = C x R
Mantenimiento de red Ethereum Privada	Técnico Instalador (ESTR.OC C1)	1,00	3,74	3,74	3,0000	11,22
SUBTOTAL M						11,22
			TOTAL COSTO DIRECTO (M)			11,22
			COSTOS INDIRECTOS		20%	2,24
ESTOS PRECIOS NO INCLUYEN EL IVA			OTROS INDIRECTOS:			
			COSTO TOTAL DEL RUBRO:			13,46
			VALOR OFERTADO:			13,46

ANEXO XII Pruebas de Transacciones en red P2P Ethereum

Aquí se ilustra el cambio del costo de transacción (fee) para el envío de 0.1 ETH dependiendo del ajuste de los parámetros de *GAS* y GWEI usando *Metamask*, un complemento del navegador Chrome para acceder a la red *Ethereum* principal, sin embargo, también es posible configurarlo para el uso con un nodo local.

Figura XV.1 Costo de transacción de 0.1 ETH y con 50 000 de gas limite

Como se puede observar el valor del "fee" depende de cuando se designe en GAS y en GWEE, siendo el gas la entidad necesaria para ejecutar contratos inteligentes, cabe destacar que el envío de ETH (*Ethe*r) de una dirección a otra es una forma de contrato inteligente.

Figura XV.2 Costo de transacción de 0.1 ETH y con 100 000 de gas limite

Las pruebas a continuación consisten en enviar ETH con varios parámetros cronometrando los tiempos de confirmación para cada transacción, para estas pruebas utilizaremos la cartera *MyEtherWallet* que es la cartera más utilizada por los usuarios de la plataforma *Ethereum*. Se analizarán los resultados utilizando la red principal y también también con el *token* KETH, una forma de ETH creada específicamente para desarrolladores; estos token están disponibles en la página GitHub oficial https://github.com/kovan-testnet/faucet, del proyecto KOVAN.

PRUEBA 1: Con Gas Limit de 21000 y con 21 Gwei:

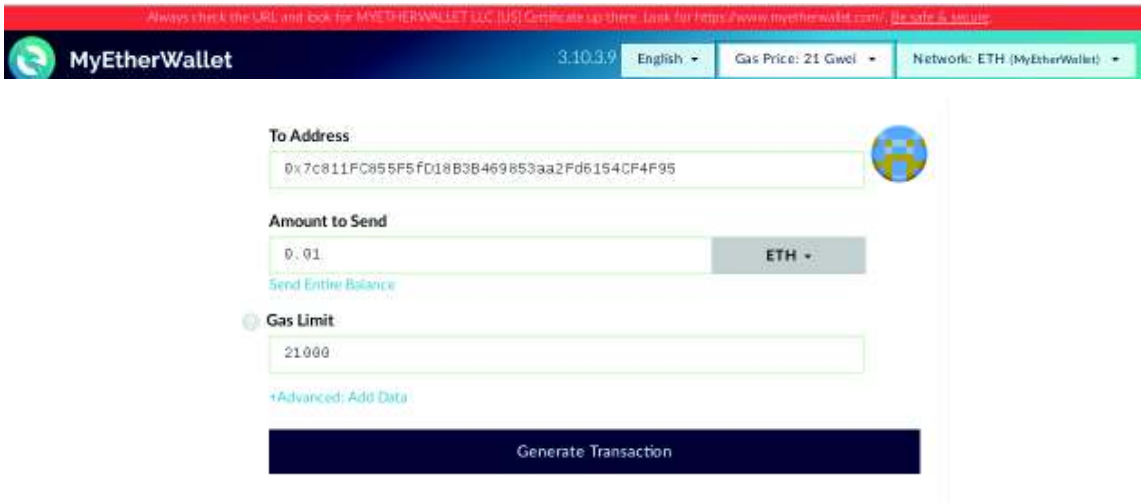

Figura XV.3 Gas Limit de 21000 y con 21 Gwei

Este envío se realizó con 6015 transacciones pendientes y 38 *peers* conectados: En la siguiente captura indica el despliegue de la página web de *MyEtherWallet*, se observa una ventana pop up indicando que la transacción inició:

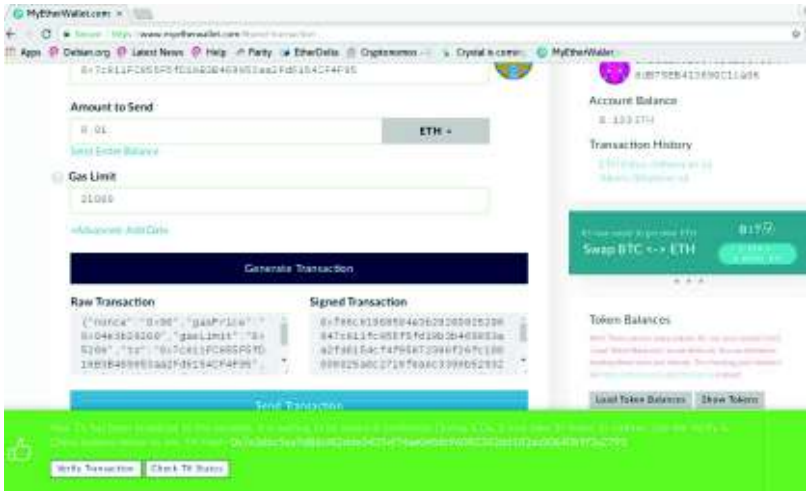

Figura XV.4 Transacción en *MyEtherWallet*,

Con un clic sobre el botón “Verify Transaction” se despliega una ventana de la página etherscan.io en la cual se observa el estado de la transacción, después de refrescar la página continuamente después de 1’ con 33’’ finalmente la transacción está confirmada en un bloque. Mientras más bloques sean minados en la red más confirmaciones tendrá esta operación.

Figura XV.5 Información de la Transacción

Una vez confirmado se confirma que se utilizaron los 21000 Gas necesarios para realizar este tipo de contrato (envío de ETH), al precio que nosotros definimos para que el “fee” total sea de $0.13 con el ETH cotizándose en el mercado a $293 al momento de realizar la prueba.

PRUEBA 2: Este envío se realizó con un “*Gas Limit*” de 210000, mientras en la red estaban pendientes 5959 transacciones y con 40 *peers* conectados. Una observación adicional para esta prueba que no se destacó en la anterior es que al momento de presionar el botón “*Verify Transaction*” la ventana de página etherscan.io despliega que la transacción está pendiente (*Pending*)

Después de 1’ con 37’’ la transacción se confirma:

Transaction Information

TxHash:	0x3066dd72795498ba0426a633f3fc41c3851f4d4f8680787fb6a0467c6105a039
Block Height:	4322632 (1 block confirmation)
TimeStamp:	1 min ago (Sep-29-2017 06:48:26 PM +UTC)
From:	0x5dde881e0f3bc23cf094a8db75eb413690c1ca06
To:	0x7c811fc855f5fd18b3b469853aa2fd6154cf4f95
Value:	0.01 Ether ($2.93)
Gas Limit:	210000
Gas Used By Txn:	21000
Gas Price:	0.000000021 Ether (21 Gwei)
Actual Tx Cost/Fee:	0.000441 Ether ($0.13)
Cumulative Gas Used:	905156
Nonce:	151

Figura XV.6 Confirmación de la transacción Prueba 2

El "fee" total fue exactamente el de la prueba anterior; lo cual confirma en primer lugar que el contrato inteligente únicamente necesita 21000 gas, y por otro lado que al no cambiar el precio GWEI que estaba configurado el resultado sería el mismo

PRUEBA 3: Se cambia el precio GWEI a 60: Con gas limit de 21000, con 5367 transacciones pendientes y 40 peers conectados:

Overview Comments

Transaction Information

TxHash:	0x3ecbd31df8d30a260e115ba0473bc111e1f0adde50c01cef6b4d5b8a809e5bcf
Block Height:	[illegible] (1 block confirmation)
TimeStamp:	51 secs ago (Sep-29-2017 07:24:28 PM +UTC)
From:	[illegible]
To:	[illegible]
Value:	0.01 Ether ($2.93)
Gas Limit:	21000
Gas Used By Txn:	21000
Gas Price:	0.00000006 Ether (60 Gwei)
Actual Tx Cost/Fee:	0.00126 Ether ($0.37)
Cumulative Gas Used:	415075
Nonce:	153

Figura XV.7 Confirmación de la transacción Prueba 3

Después de 2' y 17'' se confirma la transacción, sorprendentemente la operación tarda más a pesar de pagar una tarifa de $0.37.

PRUEBA 4: Con gas limit de 210000, 6087 transacciones pendientes y 39 peers conectados:

La transacción se confirma en 1' y 48'' con un costo de $0.37 resultado idéntico al de la prueba 3. Confirmando nuevamente que solo se consumen los 21000 gas de los 210000 que se pusieron en los parámetros de la transacción.

Transaction Information (Pending)

TxHash:	[illegible]
Block Height:	(Pending)
TimeStamp:	00 hr 00 min 04 secs ago
From:	0x5dde881e0f3bc23cf094a8db75eb413690c1ca06
To:	0x7c811fc855f5fd18b3b469853aa2fd6154cf4f95
Value:	0.01 Ether ($2.93)
Gas Limit:	210000
Gas Used By Txn:	Pending
Gas Price:	0.00000006 Ether (60 Gwei)
Actual Tx Cost/Fee:	Pending

Figura XV.8 Transacción pendiente Prueba 4

PRUEBA 5: Con 5 Gwei: Con gas limit de 21000, pendientes 5012 transacciones y 39 peers conectados:

TxHash:	0x068a2a5a37aa8f69a295b889663bf35f6469dd8e1efe3dc433b905c96edfbb0f
Block Height:	4322730 (1 block confirmation)
TimeStamp:	26 secs ago (Sep-29-2017 07:46:41 PM +UTC)
From:	0x5dde881e0f3bc23cf094a8db75eb413690c1ca06
To:	0x7c811fc855f5fd18b3b469853aa2fd6154cf4f95
Value:	0.01 Ether ($2.93)
Gas Limit:	21000
Gas Used By Txn:	21000
Gas Price:	0.000000005 Ether (5 Gwei)
Actual Tx Cost/Fee:	0.000105 Ether ($0.03)
Cumulative Gas Used:	6484270
Nonce:	155

Figura XV.9 Confirmación de la transacción Prueba 5

Después de 2’ y 38’’ la transacción se confirma, el costo fue de $0.03 siendo la más económica de todas, pero también la más lenta.

PRUEBA 6: Prueba con 210 Gwei, 5128 transacciones pendientes y 39 peers conectados.

Transaction Information {Pending}

TxHash:	0xdaa8abbef4e409b6e5fbc9a6a40454e3c9f28164da4bfb53d8989ae9463803f6
Block Height:	(*Pending*)
TimeStamp:	00 hr 00 min 02 secs ago
From:	0x5dde881e0f3bc23cf094a8db75eb413690c1ca06
To:	0x7c811fc855f5fd18b3b469853aa2fd6154cf4f95
Value:	0.01 Ether ($2.94)
Gas Limit:	21000
Gas Used By Txn:	*Pending*
Gas Price:	0.00000021 Ether (210 Gwei)
Actual Tx Cost/Fee:	*Pending*

Figura XV.10 Transacción pendiente Prueba 6

Después de 2’’ de espera no se justifica el $1.30 de costo por la transacción.

Transaction Information

TxHash:	0xdaa8abbef4e409b6e5fbc9a6a40454e3c9f28164da4bfb53d8989ae9463803f6
Block Height:	4322855 (1 block confirmation)
TimeStamp:	17 secs ago (Sep-29-2017 08:45:21 PM +UTC)
From:	0x5dde881e0f3bc23cf094a8db75eb413690c1ca06
To:	0x7c811fc855f5fd18b3b469853aa2fd6154cf4f95
Value:	0.01 Ether ($2.94)
Gas Limit:	21000
Gas Used By Txn:	21000
Gas Price:	0.00000021 Ether (210 Gwei)
Actual Tx Cost/Fee:	0.00441 Ether ($1.30)
Cumulative Gas Used:	21000
Nonce:	160

Figura XV.11 Confirmación de la transacción Prueba 6

PRUEBA 7: Con Gas Limit de 20000, 5258 transacciones pendientes y 40 peers conectados:

Figura XV.12 Error en la transacción Prueba 7

La ventana popup que antes se mostraba verde ahora se despliega con un error, este error confirma que para el tipo de contrato que se está ejecutando es necesario 21000.

PRUEBAS UTILIZANDO UN NODO LOCAL

PRUEBA 8: Usando nodo local 21000 GWEI, 21000 *Gas Limit,* 5046 y 40 peers conectados:

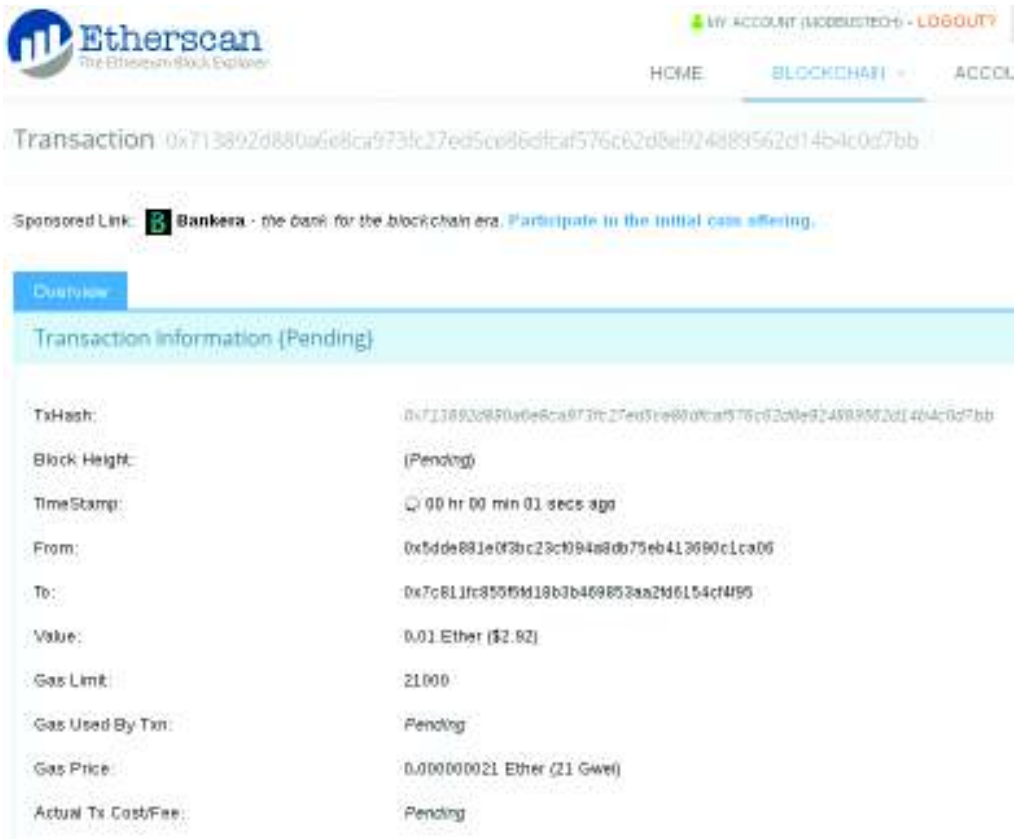

Figura XV.13 Transacción pendiente Prueba 8

Transaction Information

TxHash:	0x713892d880a6e8ca973fc27ed5ce86dfcaf576c62d8e924889562d14b4c0d7bb
Block Height:	4322791 (1 block confirmation)
TimeStamp:	34 secs ago (Sep-29-2017 08:12:48 PM +UTC)
From:	0x5dde881e0f3bc23cf094a8db75eb413690c1ca06
To:	0x7c811fc855f5fd18b3b469853aa2fd6154cf4f95
Value:	0.01 Ether ($2.92)
Gas Limit:	21000
Gas Used By Txn:	21000
Gas Price:	0.000000021 Ether (21 Gwei)
Actual Tx Cost/Fee:	0.000441 Ether ($0.13)

Figura XV.14 Confirmación de la transacción Prueba 8

Utilizando un nodo local, la transacción se resuelve en 32 segundos. Cuando una transacción se ejecuta corriendo un nodo local se presenta la siguiente información en pantalla:

```
Imported                    ( 4 txs, 5.33 Mgas, 1804.80 ms, 13.45 KiB)
Imported                    ( 183 txs, 6.71 Mgas, 3113.39 ms, 25.89 KiB)
  #3882864    5/25 peers   5 MiB chain 79 MiB db 0 bytes queue 11 MiB sync  RPC:  2 conn,  4 req/s, 184 µs
  #3882864    5/25 peers   5 MiB chain 79 MiB db 0 bytes queue 12 MiB sync  RPC:  2 conn,  5 req/s, 261 µs
Syncing                       0 blk/s    0 tx/s    0 Mgas/s      0+    0 Qed  #4322789    5/25 peers   5 MiB chain 79 M
2 MiB sync  RPC:  2 conn,  6 req/s, 151 µs
Imported                    ( 53 txs, 0.72 Mgas, 849.84 ms, 6.85 KiB)
Transaction mined (hash 713892d880a6e8ca973fc27ed5ce86dfcaf576c62d8e924889562d14b4c0d7bb)
  #3882859    4/25 peers   7 MiB chain 80 MiB db 0 bytes queue 8 MiB sync  RPC:  2 conn,  7 req/s, 264 µs
Imported                    ( 10 txs, 0.72 Mgas, 614.75 ms, 15.06 KiB)
```

Figura XV.15 Ejecución de la transacción Prueba 8

Si bien la mejora en tiempos es notable corriendo un nodo completo, a nivel de costo es mayor en lo que respecta al "*fee*" sin embargo correr un nodo en *Ethereum* requiere recursos de espacio de disco duro y de internet.

Hay que resaltar que las pruebas se realizaron mientras la red *Ethereum* no estaba bajo estrés, las transacciones ejecutadas durante una red congestionada suelen tardar varios minutos inclusive varias horas, la misma cartera *MyEtherWallet* alerta que durante las *"Initial Coin Offering ICO"* las transacciones pueden tardar horas.

Your TX has been broadcast to the network. It is waiting to be mined & confirmed. During ICOs, it may take 24 hours to confirm. Use the Verify & Check buttons below to see. TX Hash: 0x7e3d6c5ea7d86cf82dde5435ef74ae04fdb960823d2dd183aa50640b9f3a2793

Verify Transaction | Check TX Status

Figura XV.16 Congestión de la red Prueba 8

La red *Ethereum* está en constante evolución, y presenta problemas de escalabilidad inherentes a todas las cadenas de bloques con distintas tecnologías. Sin embargo, el uso de una red basada en *Ethereum* privada tiene más viabilidad por los problemas de congestión que conlleva el uso de una red pública.

A continuación, se muestran pruebas sobre una red *Ethereum* de prueba "*TestNet*" que no presenta congestión para evaluar sus resultados. Esta red de prueba se llama de KOVAN y no es la única de este tipo, esta red utiliza *tokens Ethereum* que no tienen un valor real en el mercado de las criptodivisas y *tokens* comerciales, fueron creados para que los desarrolladores prueben sus aplicaciones y contratos inteligentes.

PRUEBA 9: Envío de 0.1 ETH sobre la plataforma de prueba *Ethereum* "kovan":

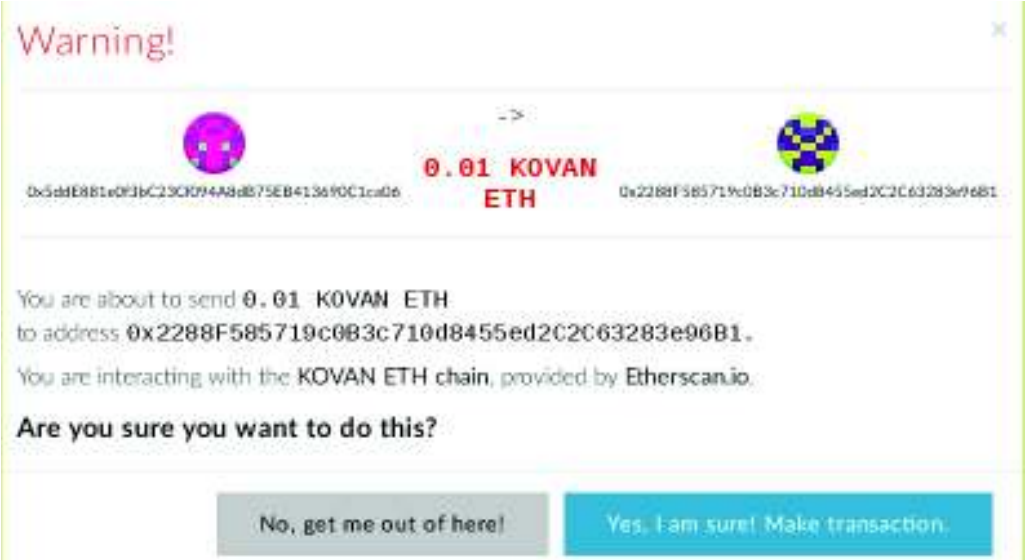

Figura XV.17 Transacción red Kovan Prueba 9

En el momento de realizar esta prueba, se verifica que tan solo hay dos transacciones pendientes, 60 peers conectados, y este valor se lo actualizamos constantemente cambia en segundos y rara vez, a la fecha de hoy 30 de septiembre del 2017, supera las 4 transacciones pendientes.

Transaction Information { Pending Confirmation }

TxHash:	0x664efbf986b9220befbf4a5ac525695f27625ec2495998f8c89ad2f67556fafa
Block Height:	(Pending)
TimeStamp:	00 hr 00 min 04 secs ago (Sep-29-2017 09:34:58 PM)
From:	0x5dde881e0f3bc23cf094a8db75eb413690c1ca06
To:	0x2288f585719c0b3c710d8455ed2c2c63283e96b1
Value:	0.01 Ether ($0.000000)
Gas Limit:	21000
Gas Used By Txn:	Pending
Gas Price:	0.000000021 Ether (21 Gwei)
Actual Tx Cost/Fee:	Pending
Cumulative Gas Used:	Pending
Nonce:	5

Figura XV.18 Transacción pendiente Prueba 9

La transacción se ejecutó en 4 segundos a un costo de $0.00, pues el token no tiene ningún valor comercial.

PRUEBA 10: La siguiente prueba plantea usar 5 Gwei, que es un valor pequeño de gas para realizar una transacción sobre esta plataforma:

Transaction Information {Pending}

TxHash:	0xa2ccf0e4c56768bad0143c460c134efd442e8c133851c9058cc438f999c1be26
Block Height:	(Pending)
TimeStamp:	00 hr 00 min 03 secs ago
From:	0x5dde881e0f3bc23cf094a8db75eb413690c1ca06
To:	0x2288f585719c0b3c710d8455ed2c2c63283e96b1
Value:	0.01 Ether ($0.000000)
Gas Limit:	21000
Gas Used By Txn:	Pending
Gas Price:	0.000000005 Ether (5 Gwei)
Actual Tx Cost/Fee:	Pending
Cumulative Gas Used:	Pending
Nonce:	6

Figura XV.21 Confirmación de la transacción Prueba 10

La transacción se ejecutó después de 11 segundos, con un consumo de gas mínimo.

ANEXO XIII Pruebas para crear el Contrato Inteligente

A continuación se presentan las pruebas del input de la transacción para crear el contrato inteligente, en la página oficial de https://ethgasstation.info/calculatorTxV.php, para calcular el valor del *Gas Price* mínimo necesario para que se ejecute la transacción.

Figura XVI.1 Input para el gas

Se empieza realizando las pruebas con los siguientes valores: Gas Price de 21 Gwei

Predictions: Gas Used = 21000; Gas Price = 21 gwei

Outcome	
% of last 200 blocks accpeting this gas price	97
Transactions At or Above in Current Txpool	71
Mean Time to Confirm (Blocks)	2
Mean Time to Confirm (Seconds)	30
Transaction fee (ETH)	0.000441
Transaction fee (Fiat)	$0.27342

Figura XVI.2 Gas Price de 9 Gwei

Predictions: Gas Used = 21000; Gas Price = 9 gwei

Outcome	
% of last 200 blocks accpeting this gas price	53
Transactions At or Above in Current Txpool	292
Mean Time to Confirm (Blocks)	29.4
Mean Time to Confirm (Seconds)	445
Transaction fee (ETH)	0.000189
Transaction fee (Fiat)	$0.11718

Figura XVI.3 Gas Price de 9 Gwei

Predictions: Gas Used = 21000; Gas Price = 8 gwei

Outcome	
% of last 200 blocks accpeting this gas price	50
Transactions At or Above in Current Txpool	193
Mean Time to Confirm (Blocks)	36.2
Mean Time to Confirm (Seconds)	475
Transaction fee (ETH)	0.000168
Transaction fee (Fiat)	$0.10366

Figura XVI.4 Gas Price de 8 Gwei

Predictions: Gas Used = 21000; Gas Price = 7 gwei

Outcome	
% of last 200 blocks accpeting this gas price	27
Transactions At or Above in Current Txpool	375
Mean Time to Confirm (Blocks)	241.6
Mean Time to Confirm (Seconds)	3658
Transaction fee (ETH)	0.000147
Transaction fee (Fiat)	$0.09114

Figura XVI.5 Gas Price de 7 Gwei

Predictions: Gas Used = 21000; Gas Price = 6 gwei

Outcome	
% of last 200 blocks accpeting this gas price	20
Transactions At or Above in Current Txpool	623
Mean Time to Confirm (Blocks)	456
Mean Time to Confirm (Seconds)	6903
Transaction fee (ETH)	0.000126
Transaction fee (Fiat)	$0.07812

Figura XVI.6 Gas Price de 6 Gwei

Predictions: Gas Used = 21000; Gas Price = 5 gwei

Outcome	
% of last 200 blocks accpeting this gas price	20
Transactions At or Above in Current Txpool	1179
Mean Time to Confirm (Blocks)	538.7
Mean Time to Confirm (Seconds)	8156
Transaction fee (ETH)	0.000105
Transaction fee (Fiat)	$0.0651

Figura XVI.7 Gas Price de 5 Gwei

Predictions: Gas Used = 21000; Gas Price = 4 gwei

Outcome	
% of last 200 blocks accpeting this gas price	20
Transactions At or Above in Current Txpool	1811
Mean Time to Confirm (Blocks)	651.2
Mean Time to Confirm (Seconds)	9859
Transaction fee (ETH)	0.000084
Transaction fee (Fiat)	$0.05208

Figura XVI.8 Gas Price de 4 Gwei

Predictions: Gas Used = 21000; Gas Price = 3 gwei

Outcome	
% of last 200 blocks accpeting this gas price	20
Transactions At or Above in Current Txpool	1812
Mean Time to Confirm (Blocks)	651.4
Mean Time to Confirm (Seconds)	9862
Transaction fee (ETH)	0.000063
Transaction fee (Fiat)	$0.03906

Figura XVI.9 Gas Price de 3 Gwei

Predictions: Gas Used = 21000; Gas Price = 2 gwei

Outcome	
% of last 200 blocks accpeting this gas price	20
Transactions At or Above in Current Txpool	1814
Mean Time to Confirm (Blocks)	651.8
Mean Time to Confirm (Seconds)	9868
Transaction fee (ETH)	0.000042
Transaction fee (Fiat)	$0.02604

Figura XVI.10 Gas Price de 2 Gwei

Predictions: Gas Used = 21000; Gas Price = 1 gwei

Outcome	
% of last 200 blocks accpeting this gas price	20
Transactions At or Above in Current Txpool	1814
Mean Time to Confirm (Blocks)	651.8
Mean Time to Confirm (Seconds)	9868
Transaction fee (ETH)	0.000021
Transaction fee (Fiat)	$0.01302

Figura XVI.11 Gas Price de 1 Gwei

Predictions: Gas Used = 21000; Gas Price = 0.1 gwei

Outcome	
% of last 200 blocks accpeting this gas price	2
Transactions At or Above in Current Txpool	1996
Mean Time to Confirm (Blocks)	2910.6
Mean Time to Confirm (Seconds)	39196
Transaction fee (ETH)	0.0000021
Transaction fee (Fiat)	$0.0013

Figura XVI.12 Gas Price de 0.1 Gwei

Predictions: Gas Used = 21000; Gas Price = 0.5 gwei

Outcome	
% of last 200 blocks accpeting this gas price	2
Transactions At or Above in Current Txpool	1996
Mean Time to Confirm (Blocks)	2910.6
Mean Time to Confirm (Seconds)	39196
Transaction fee (ETH)	0.0000105
Transaction fee (Fiat)	$0.00649

Figura XVI.13 Gas Price de 0.5 Gwei

Predictions: Gas Used = 21000; Gas Price = 0.9 gwei

Outcome	
% of last 200 blocks accpeting this gas price	2
Transactions At or Above in Current Txpool	1996
Mean Time to Confirm (Blocks)	2910.6
Mean Time to Confirm (Seconds)	39196
Transaction fee (ETH)	0.0000189
Transaction fee (Fiat)	$0.01168

Figura XVI.14 Gas Price de 0.9 Gwei

Analizando todas las pruebas para determinar el *Gas Price* más adecuado, se concluye que cuando existen múltiples de transacciones desde la misma dirección se generan transacciones pendientes (aproximadamente >100).

Todas las transacciones publicadas en la red, que manejarán un precio de Gas < 1 Gwei no se procesan inmediatamente, requieren ser supervisadas para su confirmación. Si no se confirma en 200 bloques, el precio del gas *'Safe Low'* se actualiza a un precio de Gas más alto que el que no pudo confirmar o el gas Price se actualiza al precio promedio del Gas que circula por la red.

Los valores que están en el rango de 1 a 5, trabajan en el mismo rango de 20 bloques aceptados, con 6 en 21 bloques, 7 son 30, 8 es 50 y en 9 es 63 bloques

ORDEN DE EMPASTADO

ESCUELA POLITÉCNICA NACIONAL
"CAMPUS POLITÉCNICO JOSÉ RUBÉN ORELLANA RICAURTE"

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ORDEN DE EMPASTADO

De acuerdo con lo estipulado en el Art. 27 del Instructivo para la Implementación de la Unidad de Titulación en las Carreras y Programas Vigentes de la Escuela Politécnica Nacional, aprobado por Consejo Politécnico en sesión extraordinaria del 29 de abril de 2015 y por delegación del Decano, una vez verificado el cumplimiento de formato de presentación establecido, se autoriza la impresión y encuadernación final del Trabajo de Titulación presentado por:

ALEXANDRA KARINA CARRIÓN BASANTES

Fecha de autorización: ***26 de septiembre de 2018***

M.Sc. YADIRA BRAVO
Subdecana

Alejandra P.