UNIVERSIDAD DEL VALLE DE GUATEMALA
Facultad de Ingeniería

Potencial de *Bitcoin* como método de pago y sus avances tecnológicos

Trabajo de graduación presentado por
José Gabriel Block Staackmann

para optar por el grado académico de Licenciado en
Ingeniería en Ciencia de la Computación y Tecnologías de la Información

Guatemala,
2023

UNIVERSIDAD DEL VALLE DE GUATEMALA
Facultad de Ingeniería

Potencial de *Bitcoin* como método de pago y sus avances tecnológicos

Trabajo de graduación presentado por
José Gabriel Block Staackmann

para optar por el grado académico de Licenciado en
Ingeniería en Ciencia de la Computación y Tecnologías de la Información

Guatemala,
2023

Vo.Bo.:

(f) _____

Ing. Juan Pablo Lemus

Tribunal Examinador:

(f) _____

Ing. Juan Pablo Lemus

(f) _____

MSc. Douglas Barrios

(f) _____

Ing. Roberto Chiroy

Fecha de aprobación: Guatemala, 21 de noviembre de 2023.

Agradecimientos

A mis padres, Otto Block y Patricia Staackmann. Gracias por su apoyo y confianza a lo largo de toda mi vida. Gracias a su esfuerzo y apoyo me han empujado a culminar esta etapa. A Juan Lemus. Gracias por asesorarme en este proceso de inovación y aprendizaje. Gracias por su ayuda con la toma de desiciones. A Maria Jimena. Gracias por caminar a mi lado durante estos años. Gracias por su constante apoyo y aliento durante el proceso de este proyecto. A mis amigos de la universidad. Gracias por su apoyo y su compañerismo durante este tiempo.

Índice

Lista de figuras

Resumen

El presente trabajo de graduación busca resolver la incertidumbre que existe con respecto al concepto de *Bitcoin*, junto con una tecnología emergente llamada *Lightning Network*. La *Lightning Network* (*LN*), al funcionar como método de pago, ha abierto puertas para la aceptación de *Bitcoin* en diversos modelos de negocio. Este efecto se está manifestando principalmente en Latinoamérica. Por ende, resulta esencial comprender a fondo los conceptos que respaldan el funcionamiento de estas tecnologías para fomentar la confiabilidad y popularidad de un bien descentralizado y futuramente estable. El proceso de investigación reveló una carencia de material educativo relacionado con estas tecnologías, especialmente en español. Se han presentado numerosas críticas al método de pago *LN*, basándose en la suposición de que su manejo de *bitcoin* es poco transparente.

Como solución, se propone una guía interactiva en español que permita al usuario profundizar en su entendimiento del tema. Esta guía priorizará que el usuario lea lo más importante acerca de ambas tecnologías, basándose en criterios literarios y la opinión de expertos que trabajan con *LN* y *Bitcoin*. El objetivo es facilitar el entendimiento y aceptación de *Bitcoin* como un bien transaccional confiable.

Abstract

The purpose of this graduation project is to solve the uncertainty around the functioning of Bitcoin along with the emergent technology: Lightning Network. Thanks to LN, the acceptance of Bitcoin as a payment method has increased in business like restaurants. This impact is growing, especially in Latin America, and, due to lack of education and misinformation regarding these technologies and their performance, there have been many indictments against this payment method, assuming it is not Bitcoin.

CAPÍTULO 1

Introducción

Hoy en día, *Bitcoin* es una criptomoneda bastante conocida; actualmente es poco común encontrar a alguien que no haya escuchado al respecto. Esta es la primera criptomoneda en ser creada desde el anonimato, de manera que tiene valor descentralizado, único, no duplicable e intercambiable entre otras divisas. Además, tiene la capacidad de hacer transacciones irreversibles *peer to peer*. A raíz de *Bitcoin*, surgió una tecnología llamada *Lightning Network*, la cual es una solución parcialmente *off-chain* que permite realizar microtransacciones inmediatas, con cuotas más bajas al compararse con una transacción *on-chain*. Explicado de manera sencilla, *LN* (*Lightning Network*) es una red de nodos interconectados de los cuales sus conexiones representan un balance de *Bitcoin* el cual, transacción por transacción, mueve el balance al nodo receptor. Estas conexiones color rojo representan canales (Fig. 1). Al cerrar un canal se pacta el balance final entre los nodos conectados y se carga al blockchain de bitcoin con una transacción *on-chain*.

En el transcurso de este trabajo de graduación se presentará el alcance del *Bitcoin* a través de extensiones como *Lightning Network* con su funcionamiento. Luego se demostrará su alcance con diferentes casos de uso y la herramienta *LNURL* la cual es un plug-in que ha traído mucha mejora de experiencia de usuario, volviendo mucho más simple y agradable el uso de *LN*. La implementación que se utilizará de *LN* será *LND*, un opensource software que define a un nodo que cumple con el protocolo de Lightning. Se harán demostraciones de código ejemplo e imágenes para comparar el flujo de *UX* al implementar *LNURL* y al usar simplemente *LN* o el método de pago *on-chain* de *Bitcoin*. Se explicarán casos de uso que expliquen las facilidades que incluyen cada una de las extensiones y que amplían el alcance de *Bitcoin* como un bien transaccional.

Se considera a *Bitcoin* como un bien mucho más versátil y me gusta la idea de que haya un método de pago descentralizado disponible para todo aquel que tenga internet y ganas de involucrarse. Este trabajo se desarrollará de manera que se entienda el concepto de *Bitcoin*, *Lightning Network* y *LNURL*(cada una con sus respectivos ejemplos). También, que se expliquen las diferencias entre *on-chain* y una transacción vía *LN*. Luego se hablará a más detalle de ciertas dificultades de *UX* que se pueden dar con *LN* y cómo resolverlas con *LNURL*. Se realizará y explicará el código de ejemplo para que se pueda comprobar el funcionamiento de *LN* y *LNURL*. Por lo tanto, esto es una guía para todo aquel interesado en entender o incluso desarrollar *Lightning Network*.

CAPÍTULO 2

Objetivos

2.1. Objetivo general

Explicar la conexión entre *Bitcoin* y *Lightning Network* por medio de una guía interactiva para demostrar su alcance tecnológico.

2.2. Objetivos específicos

- Definir qué es *Bitcoin* y cuál es su alcance tecnológico.
- Demostrar qué es *Lightning Network* y su alcance tecnológico.
- Dar a conocer las mejoras que *LNURL* puede proveer a un negocio con *Bitcoin* vía *LN*.
- Crear una herramienta educativa e interactiva para comprender la relación entre *Bitcoin* y *Lightning Network*.

CAPÍTULO 3

Justificación

El propósito de este trabajo de graduación es facilitar la visualización del alcance del bien digital conocido como bitcoin. Uno de los mayores problemas que existen con *Bitcoin* es que, la mayoría de los usuarios no tienen un conocimiento claro del mecanismo de esta red. También desconocen de los avances tecnológicos que han surgido junto con *Bitcoin*. En este caso se hablará de *Lightning Network* y cómo esta nueva implementación cambia bastante la perspectiva que inicialmente se le tenía a *Bitcoin*. En una encuesta de 100 participantes hispanohablantes, el 95 % considera que saben suficiente respecto a *Bitcoin*, pero 79 % desconoce de *Lightning Network*, una tecnología de alto impacto a la criptomoneda. Otro punto importante de mencionar es que para probar *Bitcoin* se requiere invertir económicamente para hacer transacciones y entender cómo funciona, sin embargo, esto no es factible para todas las personas interesadas en aprender respecto al tema. Cabe mencionar que en el proceso de investigación se pudo notar que los recursos más enriquecedores de los temas estaban explicados únicamente en ingles. Se sabe que El Salvador es el primer país en adoptar a *Bitcoin* como una moneda de curso legal y al ver los resultados de la encuesta, se puede notar la falta de material educativo al accesso de todos los hispanohablantes. Crear material educativo, interactivo y accesible para hispanohablantes motivará a profundizar en el conocimiento de bitcoin para poder entender el alcance tecnológico de la relación entre *Bitcoin* y *Lightning Network*. Por lo tanto, los usuarios tendrán una idea de las capacidades, procesos y limitaciones más importantes de *Bitcoin* con *Lightning Network*, para que puedan hacer uso de esta tecnología comprendiendo su funcionamiento. Seguramente el primer usuario de un carro tuvo sus miedos y dudas al experimentar con el primer modelo. Con este proyecto se busca resolver dudas comunes y mitigar miedos respecto a *Bitcoin* de una forma dinámica y escalable.

CAPÍTULO 4

Marco teórico

4.1. Blockchain

4.1.1. ¿Qué es?

Un *blockchain* o cadena de bloques es un libro de contabilidad inmodificable y compartido que facilita el proceso de registro de transacciones y seguimiento de activos en una red empresarial. Un activo puede ser tangible (una casa, un coche, dinero en efectivo, tierra) o intangible (propiedad intelectual, patentes, derechos de autor, marca). Prácticamente cualquier cosa de valor puede ser rastreada y comercializada en una red *blockchain*, de modo que se reducen el riesgo y los costes para todos los involucrados. [1]

4.2. *Bitcoin*

4.2.1. ¿Qué es?

Bitcoin representa una innovación en el dinero digital al ser descentralizado y seguro gracias a la criptografía y la tecnología *blockchain*. Es una forma de dinero en línea que está cambiando la forma en que entendemos las transacciones financieras y la propiedad de activos digitales.[2][3]

Bitcoin es un bien digital que utiliza un protocolo y tecnología *peer-to-peer* para permitir transacciones en línea de manera rápida, segura y sin fronteras. A diferencia de las monedas tradicionales, el *bitcoin* es completamente virtual, no existen monedas físicas. Se almacena en billeteras digitales y se transfiere mediante claves criptográficas. *Bitcoin* opera en una red descentralizada, sin un servidor central o entidad de control. Los *bitcoins* se crean a través de un proceso llamado "minería", que verifica y registra las transacciones en la red. El protocolo de *Bitcoin* incluye algoritmos que regulan la minería y limitan la cantidad total de *bitcoins* que se crearán, lo que lo hace deflacionario a largo plazo.[2][3]

Bitcoin es la primera aplicación de una tecnología que combina una red *peer-to-peer* descentralizada, un registro público de transacciones (la cadena de bloques), reglas de consenso y un algoritmo

de Prueba de Trabajo para alcanzar un consenso global. Antes de *Bitcoin*, hubo intentos de crear monedas digitales centralizadas, pero fueron vulnerables a ataques gubernamentales y *hackers*.[2][3]

4.2.2. Ventajas de *Bitcoin*:

- Descentralización: *Bitcoin* opera en una red descentralizada de nodos, lo que lo hace resistente a la censura y al control de cualquier entidad única, como un gobierno o una empresa.[2]
- Seguridad: La red *Bitcoin* utiliza técnicas criptográficas para garantizar la seguridad de las transacciones, lo que la hace altamente segura y resistente a manipulaciones.[2]
- Oro digital: *Bitcoin* a menudo se compara con el oro como reserva de valor. Algunos inversores lo ven como una protección contra la inestabilidad económica y la inflación.[2]
- Accesibilidad global: *Bitcoin* puede ser utilizado por cualquier persona con una conexión a *Internet*, lo que lo hace accesible para personas en regiones con acceso limitado a servicios bancarios tradicionales.[2]
- Menores tarifas de transacción: Las transacciones de *Bitcoin* pueden tener tarifas más bajas en comparación con los sistemas financieros tradicionales, especialmente para transacciones internacionales.[2]
- Programabilidad: La tecnología subyacente de *Bitcoin*, la cadena de bloques, se puede utilizar para diversas aplicaciones programables más allá de la moneda, como contratos inteligentes.[2]

4.2.3. Desventajas de *Bitcoin*:

- Volatilidad: El precio de *Bitcoin* es conocido por su extrema volatilidad, lo que puede convertirlo en una inversión arriesgada.[2]
- Escalabilidad limitada: La capacidad de procesamiento de transacciones de *Bitcoin* es limitada, lo que puede llevar a la congestión en momentos de alta demanda.[2]
- Consumo de energía: El mecanismo de consenso de Prueba de Trabajo (PoW) utilizado por *Bitcoin* requiere un consumo significativo de energía, lo que ha generado preocupaciones medioambientales.[2]
- Incertidumbre regulatoria: El entorno regulatorio para *Bitcoin* varía ampliamente de un país a otro, lo que crea incertidumbre para usuarios y empresas.[2]
- Transacciones irreversibles: Las transacciones de *Bitcoin* son irreversibles, lo que significa que una vez confirmadas, no se pueden deshacer. Esto puede ser una desventaja en casos de fraude o error.[2]
- Falta de privacidad: Si bien las transacciones de *Bitcoin* son seudónimas, no son completamente privadas y es posible rastrear el historial de transacciones.[2]

4.3. Lightning Network

4.3.1. ¿Qué es?

La *Lightning Network* es una red que permite transacciones rápidas y económicas en criptomonedas como *Bitcoin* y Litecoin. Opera fuera de la cadena principal, lo que significa que las transacciones

no se registran en la *blockchain* principal cada vez. En lugar de eso, los usuarios pueden abrir canales de transacción con otros usuarios mediante contratos inteligentes. Estos canales funcionan como libros de contabilidad privados, lo que permite transacciones rápidas y privadas. Los saldos se actualizan entre las partes y sólo se registran en la *blockchain* principal cuando se cierra el canal. Esto hace que las transacciones sean extremadamente rápidas, sin necesidad de esperar confirmaciones de bloques. [4][5]

4.3.2. Ventajas de la *Lightning Network*:

- Escalabilidad: La *Lightning Network* aborda el problema de la escalabilidad en *Bitcoin* al permitir transacciones fuera de la cadena principal. Esto reduce la congestión en la cadena y permite que las transacciones sean más rápidas y económicas. [5]
- Micropagos: La *Lightning Network* es ideal para micropagos, ya que permite enviar cantidades muy pequeñas de *Bitcoin* de forma gratuita. Las comisiones de las transacciones normales en la cadena principal pueden hacer que los micropagos no sean viables.[5]
- Privacidad: La *Lightning Network* ofrece un alto grado de privacidad. Los usuarios no necesitan revelar sus canales a la red en general, lo que aumenta la confidencialidad de las transacciones. Además, los detalles de las transacciones en un canal privado son conocidos sólo por las partes involucradas.[5]
- Usabilidad: Aunque *Bitcoin* puede ser complicado para principiantes, los monederos pueden simplificar la experiencia. *Lightning Network* está trabajando en mejoras para hacerla más accesible a través de aplicaciones para teléfonos inteligentes y reducir las barreras de entrada.[5]

4.3.3. Desventajas de la *Lightning Network*:

- Comisiones iniciales: Aunque las transacciones dentro de un canal de *Lightning* son gratuitas una vez abierto, los usuarios deben pagar comisiones para abrir y cerrar canales. Esto puede desalentar a algunos usuarios, especialmente para transacciones de bajo valor.[5]
- Complejidad: Utilizar la *Lightning Network* puede ser más complicado que las transacciones regulares en la cadena principal de *Bitcoin*. Los usuarios deben comprender cómo funcionan los canales y cómo administrarlos.[5]
- Interoperabilidad: No todos los servicios y billeteras son compatibles con la *Lightning Network*, lo que limita su adopción. Esto podría cambiar con el tiempo a medida que más servicios la integren.[5]
- Limitaciones en la usabilidad: La configuración de un cliente de *Lightning Network* y la apertura de canales pueden ser procesos complicados para los nuevos usuarios, lo que puede generar confusión y retrasos en la realización de pagos.[5]
- Restricciones de liquidez: La capacidad de realizar transacciones en *Lightning Network* está limitada por la cantidad de fondos bloqueados en un canal. Las rutas de pago también pueden estar limitadas por la capacidad de los canales intermedios, lo que afecta negativamente la flexibilidad en la transferencia de fondos.[5]
- Hubs centralizados: Existe la preocupación de que la red de *Lightning Network* pueda facilitar la creación de entidades centralizadas o *hubs* que manejan una gran cantidad de liquidez. Esto podría debilitar el sistema, interrumpir relaciones entre pares y aumentar el riesgo de censura, ya que los pagos significativos tendrían que pasar por estos *hubs*.[5]

4.4. Nodo

La definición de un nodo puede variar significativamente según el contexto en el que se utiliza. Cuando se trata de redes informáticas o de telecomunicaciones, los nodos pueden ofrecer fines distintos, ya sea como un punto de redistribución o un punto final de comunicación. Por lo general, un nodo consiste en un dispositivo de red físico, pero hay algunos casos específicos en los que se usan nodos virtuales.[6]

En pocas palabras, un nodo de red es un punto en el que se puede crear, recibir o transmitir un mensaje. A continuación, analizaremos los diferentes tipos de nodos de *Bitcoin*:

4.4.1. Nodos completos (Full Nodes)

Almacenan una copia completa y actualizada de la *blockchain* de *Bitcoin*. Validan y verifican todas las transacciones y bloques en la red. Proporcionan seguridad y descentralización a la red. Pueden transmitir nuevas transacciones y bloques a la *blockchain*. Requisitos mínimos para ejecutar un nodo completo incluyen una computadora con espacio en disco, memoria RAM y una conexión a *Internet* de alta velocidad.[6]

4.4.2. Nodos de escucha (Supernodos)

Son nodos completos públicamente visibles. Actúan como puntos de redistribución de datos y puentes de comunicación en la red. Se ejecutan las 24 horas del día y tienen múltiples conexiones establecidas con otros nodos. Requieren más poder de cómputo y una mejor conexión a *Internet* en comparación con nodos completos ocultos.[6]

4.4.3. Nodos mineros

Minan nuevos bloques de *Bitcoin* y compiten por recompensas. Pueden trabajar en solitario o en grupos de minería (pools). Los grupos de minería sólo requieren que el administrador ejecute un nodo completo.[6]

4.4.4. Clientes ligeros o clientes *SPV* (*Simplified Payment Verification*)

No almacenan una copia completa de la *blockchain*. Verifican transacciones utilizando información proporcionada por otros nodos completos. Las utilizan muchas carteras de criptomonedas para verificar transacciones sin descargar la *blockchain* completa.[6]

4.4.5. *LND(Lightning Network Daemon)*

LND es una implementación completa de un nodo de la red *Lightning*. Puede funcionar con diferentes servicios de cadena (como *btcd*, *bitcoind* y *neutrino*) y utiliza las bibliotecas de *Bitcoin* del conjunto btcsuite. *LND* también ofrece una serie de bibliotecas aisladas y reutilizables relacionadas con la red *Lightning*. En su estado actual, *LND* puede crear canales, cerrar canales, gestionar todos los estados del canal, mantener un gráfico de canales autenticado y validado, encontrar rutas de pago, reenviar pagos entrantes, enviar pagos salientes de forma encriptada y actualizar las tarifas

anunciadas. También es capaz de gestionar canales de forma automática a través de la función de *autopilot*. [7]

4.5. *LNURL*

4.5.1. ¿Qué es?

LNURL es un protocolo sobre *HTTP* que facilita la comunicación y coordinación en la red *Lightning*. Es de código abierto y consta de 20 documentos llamados textitLUD que describen cómo implementar el protocolo en billeteras y servicios. El flujo típico de *LNURL* implica escanear un código QR con una billetera LN. La billetera realiza una solicitud a una URL que se obtiene del código. El servidor responde con información y acciones a realizar. La billetera y el servidor pueden interactuar en la red *Lightning* en función de estas instrucciones. *LNURL* simplifica la comunicación en la red *Lightning*, mejorando la experiencia del usuario y permitiendo a los desarrolladores crear características innovadoras. [8]

CAPÍTULO 5

Antecedentes

Este trabajo tiene relación con el proyecto de graduación del exalumno Sebastian Arriola, que explica *LN* y cómo configurar un nodo. Con ese proyecto podrá montar su propio nodo y experimentar todas las características que se hablan en este proyecto, con *bitcoin* real.

CAPÍTULO 6

Metodología

6.1. Administración del proyecto

El proyecto se comenzó con un listado de necesidades y se escogieron las herramientas que permitieran hacerlo de forma eficiente. Se escogió un controlador de versiones llamado *Github* con motivos de poder llevar un órden de los avances. Se crearon dos repositorios, un repositorio con un template de *Wordpress* para el comienzo de la guía y un repositorio para el código con las implementaciones de *Lightning Network*.

La creación y priorización de tareas en cada repositorio se obtenía cada vez que se lograba un *milestone* mediante retroalimentación. El criterio que se usó con los entrevistados tenía un requerimiento de conocimiento previo de la tecnología, que supieran usar *Lightning Network* para tener comentarios enfocados en el contenido y considerar si es necesario o no agregar, cambiar, quitar información o dinámicas. Parte del personal con el que se trabajó fue con programadores y otros puestos de la empresa IBEX Mercado, una empresa que provee infraestructura para transacciones de *Bitcoin* con LN. También se trabajó con conocidos interezados en *Bitcoin*.

6.2. *UI / UX*

6.2.1. *User persona*

El proyecto inició con un estudio de mercado, una encuesta de 130 participantes. En una pregunta de voto multiple, el 45 % prefieren enterarse de *Bitcoin* por un video, 34 % por una guía o tutorial y 27 % por un artículo. El 55 % de los encuestados investigarían respecto a *Bitcoin* en su celular, 32 % en su computadora y 13 % en una tablet. Los intereses más destacados en el caso de *Lightning Network* son: su velocidad y eficiencia al hacer una transacción. En el caso de *Bitcoin* es: el tiempo que toma cada transacción, por qué toma tanto tiempo una transacción. Por qué a pesar de que la transacción ya está en el *blockchain*, no se refleja en la billetera, etc. A raíz de estos resultados se decidió hacer una guía dinámica que explique la conexión de *Bitcoin* con dos nuevas tecnologías que han mejorado la experiencia de usuario de *Bitcoin*.

Se desarrolló un *user persona* donde se describe al usuario arquetipo para el cual se desarrolló

esta guía.

Figura 6.1: *User persona*: lector

6.2.2. Paleta de colores

Se propuso una paleta de colores que brindan al usuario una sensación de sofisticación, combinado con colores encendidos que brindara dinamismo y alegría. (6) Se eligió el contraste entre blanco y negro como colores predominantes en el fondo de toda la guía. Este juego de colores se vió principalmente determinado por el tipo de texto en cada diapositiva. Para los colores acento, se utilizó el amarillo como color primario y el naranja y morado como colores acento secundarios. El color amarillo se utiliza específicamente en las ilustraciones de la criptomoneda *Bitcoin*. Este color transmite alegría y, además, se relaciona con el oro, lo cual da una percepción de valor e importancia al tema. Los colores morado y naranja se utilizan a lo largo de las gráficas y diferentes ilustraciones. Además, el color morado es el color complementario del amarillo, lo cual genera armonía y movimiento. El color naranja, en la psicología del color, se relaciona directamente con la tecnología, unificando la guía con el tema. (6)

Figura 6.2: Paleta de colores

6.2.3. Diagrama de flujo de la guía

6.2.4. Prototipo

Se realizó un prototipo gráfico de la guía en la cual se detalló preliminarmente la distribución de los elementos gráficos y textuales en cada página. También, se definió el sistema de acordeón para desglosar cada tema. Se eligió en el prototipo el título de la guía y la paleta de colores.

Figura 6.3: Prototipo creado

6.3. Guía dinámica

6.3.1. Investigación

El desarrollo de la guía se comenzó con una investigación. Se buscaron formas de publicar una guía, que facilitaran el desarrollo y tuvieran una amplia capacidad de edición, pero principalmente una audiencia extensa. Inicialmente se pensó usar *Medium*: una aplicación web con un editor de texto que permitiera desarrollar la guía por su gran audiencia. Al comenzar a utilizarlo, se pudo prever que las funcionalidades que tenía el editor de texto no bastaban para cumplir con el diseño final que se tenía. Por lo tanto, se decidió usar *Wordpress*, ya que este también tiene una audiencia amplia y sus capacidades de edición y dinamismo con el contenido son casi ilimitadas. Se indagó más con respecto a *Wordpress*, se pudo encontrar una herramienta de desarrollo con *Wordpress* que permitía trabajar localmente en el recurso y tenía compatibilidad con *github* llamada *Local*. Lo más útil de esta herramienta es que el programa se inicializa localmente con el uso de un solo botón, esto se encargó casi por completo del manejo de dependencias. Lo que facilitó bastante poder comenzar a programar la guía.

Para el código que proveerá el uso de *Lightning Network* local se decidió usar *Python* ya que es el lenguaje de programación más conocido y usado actualmente. Junto con la implementación de *Python* se utilizará una herramienta llamada *Polar*, que permite montar una red de nodos de *Lightning Network* como por ejemplo:

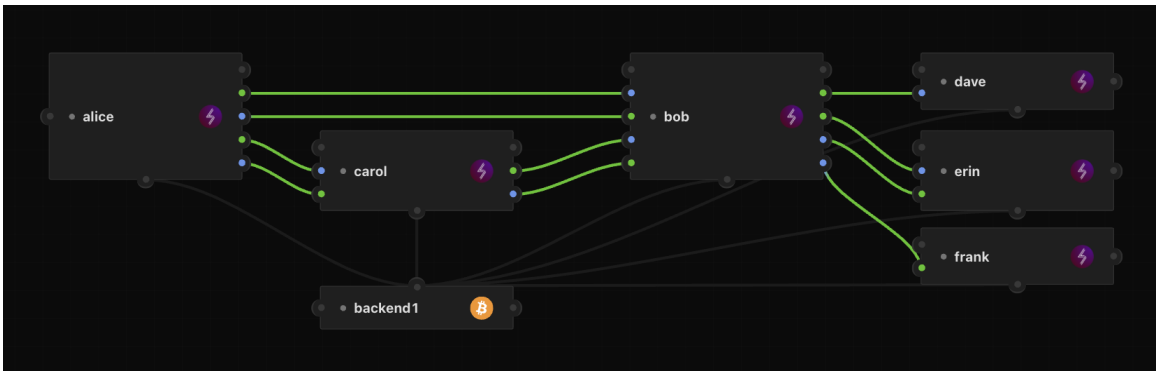


Figura 6.4: Red de nodos de LN

Es importante notar en la imagen que se tiene una conexión entre nodos de *LND*, se decidió usar este tipo de nodos debido a que son el software de nodos más usado en la *Lightning Network* y por lo tanto tiene bastante documentación que incluso ayuda a entender el protocolo de *Lightning Network*. Un tema negativo de *Polar* es que es dependiente de *Docker*, por lo tanto cada usuario que use este sistema tendrá que instalar *Docker* también.

6.3.2. Diseño de código

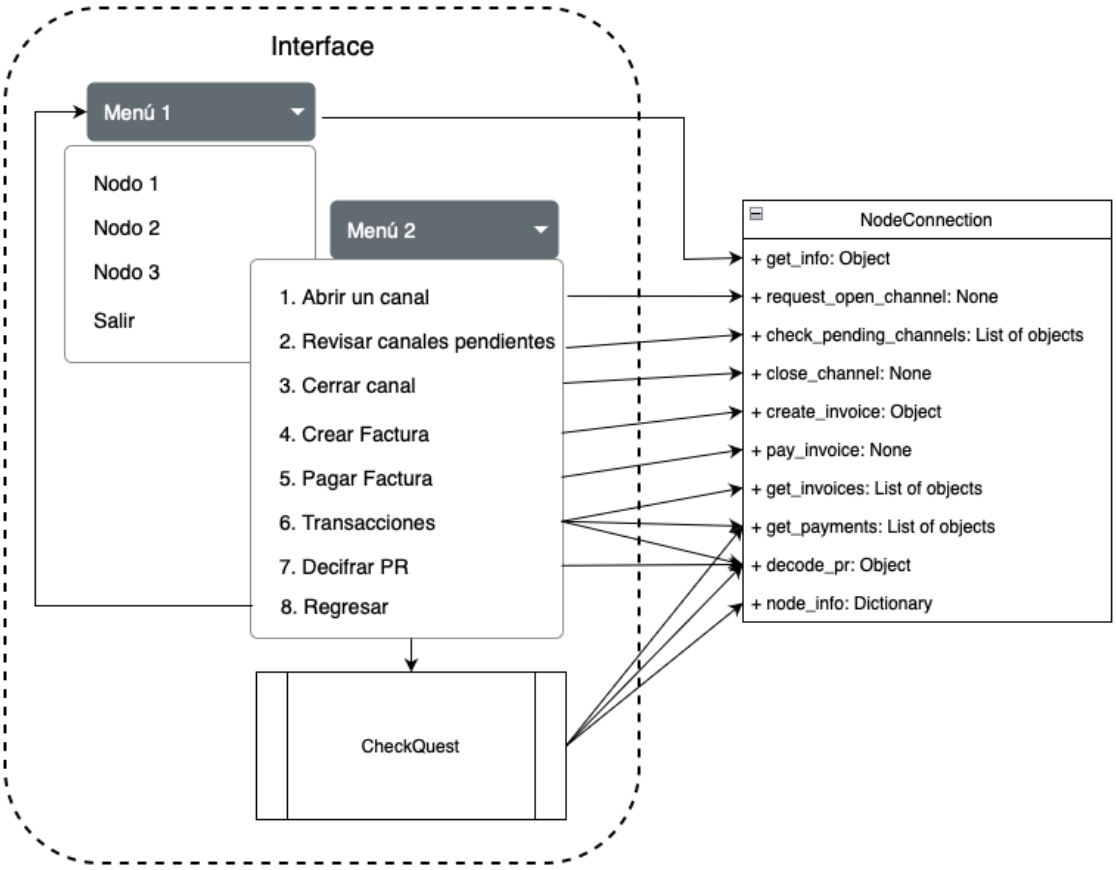


Figura 6.5: Diseño del código para prueba de LN local

Pues el concepto inicial es tener un administrador de nodos. En el cual inicialmente se escoge a qué nodo conectarte y luego qué acción hacer con ese nodo. Con esta interfaz se piensa construir una historia con un desafío agregado, en la cual se ayuda a un negocio a armar un flujo de pagos entre clientes, negocio y proveedor. Se incluyó un proceso llamado *CheckQuest* para revisar si el desafío fue completado, para pensar agregar una extensión de la historia o incentivo para que el usuario la complete.

6.3.3. Desarrollo

Inicialmente se hizo un programa que conectara con un nodo y demostrara su información. Para esto se usó una librería de *gRPC* de python para completar con los requerimientos de *LND* y también se hizo uso de un archivo .proto que al ejecutarse genera un API para acceder a todas las funcionalidades de *LND*. A continuación se muestra el primer pedazo de código que define la conexión con un nodo de *LND* por medio de una llamada al servidor *gRPC*.

```
#-------------------------------------------------------------
# Esta variable de entorno es usada por gRPC para especificar que el servidor
# debe usar un conjunto de algoritmos de seguridad alto en protocolos SSL/TLS
# con uso de certificados ECDSA para la autenticación.
os.environ["GRPC_SSL_CIPHER_SUITES"] = 'HIGH+ECDSA'
#-------------------------------------------------------------------------------

# Es un certificado TLS autofirmado que debe ser usado por los clientes que desean
#  conectarse a un servidor LND.
cert = open(os.path.expanduser(node["cert"]), 'rb').read()
#-------------------------------------------------------------------------------

#Aquí se lee el macaroon de cada nodo que esta localmente guardado en el dispositivo que
#corre el nodo, un macaroon es un token criptográficamente verificable.
macaroon_bytes = open(os.path.expanduser(node["admin_macaroon"]), 'rb').read()
macaroon = codecs.encode(macaroon_bytes, 'hex')
###############################################################################

#Funcións que agregan el macaroon como metadata y el cert como las credenciales para el canál
# SSL(Secure Sockets Layer) a cada petición que haga este programa al servidor del nodo.
metadata = [('macaroon', macaroon)]
auth_credentials = grpc.metadata_call_credentials(lambda context, callback: callback(metadata, None))
ssl_credentials = grpc.ssl_channel_credentials(cert)
channel_credentials = grpc.composite_channel_credentials(ssl_credentials, auth_credentials)
channel = grpc.secure_channel(node["channel"], channel_credentials)
#-------------------------------------------------------------------------------------------------

# Se crea un objeto que nos servirá como canal seguro de
# comunicación y accesso para poder hacer peticiones al
# servidor del nodo.
stub = lnrpc.LightningStub(channel)
#-----------------------------------------------------
```

Figura 6.6: Código que explica conexión con un nodo *LND*

Con esta conexión armada, se comenzó a hacer una investigación en la documentación de *LND* para poder escoger qué funciones usar para lo que se quería hacer. Como se muestra en la figura de diseño de código 6.5 se usan un total de diez funciones de las cuales nueve son para uso específico del nodo. A continuación detallaré para qué sirve cada una de ellas.

6.3.4. Funciones

- *get_ info*: Extrae la información del nodo, su alias, su versión y más.
- *request_ open_ channel*: Es una petición en la cual se envía una transacción de *Bitcoin* para la apertura del canal y se espera a que se minen "n" bloques para confirmar la apertura del canal.
- *check_ pending_ channels*: Es una petición para revisar los canales que aún no han sido exitosamente creados o eliminados. Retornará una lista de objetos según el estado pendiente del canal. Puede ser un canal que aún no se ha conectado con el nodo y está en espera a que se minen más bloques para que la transacción sea aceptada.
- *close_ channel*: Petición que busca cerrar un canal por medio de su identificador llamado *channel point*, esta realiza una transacción de *Bitcoin* de cierre de los saldos finales del canal.
- *create_ invoice*: Es una petición que permite hacer un cobro. Esta tiene bastantes variaciones como parámetros, pero el único parámetro que no puede faltar es un monto. Retorna un string codificado al cual se le llama *invoice* o *payment_ request*.

- *pay_ invoice*: Esta petición requiere obligatoriamente de un *invoice*, el string con la información del cobro y lo paga.
- *get_ invoices*: Esta retorna todos los cobros que se han realizado en el nodo con información importante como por ejemplo si ya fueron pagados o no y si ya vencieron, ya que todo *invoice* tiene un tiempo de caducidad.
- *get_ payments*: Retorna todos los pagos que ha hecho el nodo, con su estado actual y su información.
- *decode_ pr*: Esta función es importante ya que con esta función se puede ver el contenido de un *invoice*, esta función se usa en todas las billeteras para poder ver la información del cobro antes de pagarlo.

Debido a que se decidió trabajar con *Wordpress* para desarrollar la guía, se procedió a realizar la instalación de *Wordpress* en un entorno local por medio de la herramienta de *Local WP*, una herramienta que facilita la creación de un entorno local tanto de *PHP* como de la base de datos *MySQL* que utiliza *Wordpress* nativamente. Se creó un proyecto de *Wordpress* con la última versión hasta la fecha (versión 6.2), así como la última versión de *MySQL* (versión 8.0.19) como se puede observar en la siguiente figura:

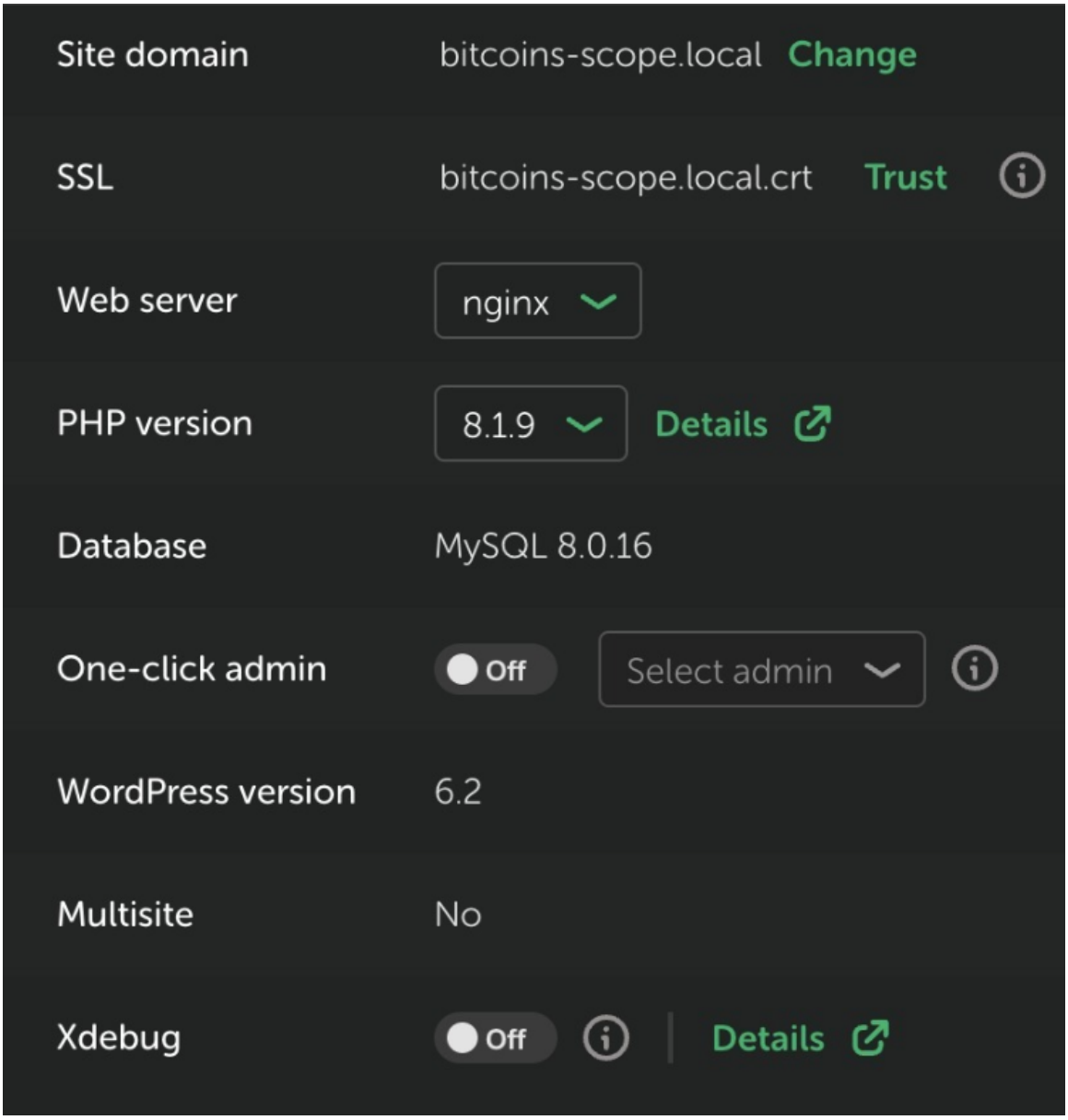


Figura 6.7: Especificación configuración proyecto *Wordpress*

Posterior a la creación del proyecto, se procedió a la creación de un tema personalizado, para no utilizar ninguna plantilla que ofrece *Wordpress* y poder proporcionar un nivel de personalización mayor. El tema creado se desarrolló con archivos de extensión de *PHP* para utilizar los *hooks* que proporciona *Wordpress*, sin embargo, la estructura y estilos son creados con *HTML*, *CSS* y *JavaScript*.

CAPÍTULO 7

Resultados

7.1. Guía alpha

El resultado de la guía fue un documento interactivo, dinámico y compacto con información educativa acerca de la conexión entre *Bitcoin* y *Lightning Network*. La guía explica, paso a paso, de manera gráfica y teórica dicha dinámica. El objetivo de la guía es que cada lector pueda ir, a su ritmo, comprendiendo *Bitcoin* y *Lightning Network*. Al final, a modo de comprobación, se desarrolló un desafío en el cuál aquel usuario interesado pueda poner a prueba sus conocimientos y recibir una pequeña remuneración por su logro.

Figura 7.1: Primera vista de la guía

Para la información presentada en la guía se usaron varios recursos: artículos[9][10][11][12], videos[13][14][15], documentación [16] y exploradores de bloques[17].

A continuación se podrán observar las extensiones de la guía, empezaremos con las de *Bitcoin*:

Conoce Más

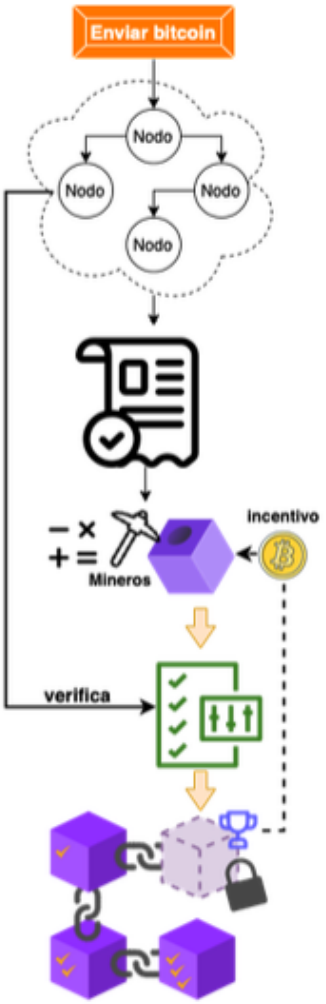
El código open-source de Bitcoin es el programa principal que representa a un nodo. Cada vez que alguien descarga y ejecuta el código de Bitcoin, agrega un nodo a la red. Por lo tanto la red de Bitcoin es un conjunto de nodos que configurados en dispositivos y son los encargados de procesar, verificar y propagar transacciones.

Junto con los nodos trabajan también los mineros, estos son los encargados de ejecutar uno o multiples dispositivos que pasan alta demanda computacional con el fin de resolver un problema matemático complejo, a este acto se le conoce como proof-of-work. Los nodos comprueban que el resultado sea correcto, todo con el de agregar un nuevo bloque a la cadena de bloques de Bitcoin. Claro que estos mineros tienen insentivo para realizar tal tarea, al final se les entrega el total de tarifas de todas las transacciones del bloque minado mas el bitcoin nuevo que se hace al crear un bloque.

Figura 7.2: Primera extensión de la explicación de *Bitcoin*

Conoce Más

¿Qué pasa en una transacción de Bitcoin?



1.
Se publica la transacción de una billetera digital con la dirección del receptor, su cantidad de bitcoin y una tarifa a la red Bitcoin.

2.
Los nodos comunican la transacción con los mineros.

3.
Los mineros crean un nuevo bloque y lo llenan con transacciones por verificar.

4.
Simultaneamente los mineros compiten por resolver un problema matemático de hashing. El minero ganador publica el bloque.

5.
Los nodos verifican que la transacción cumpla con las reglas del protocolo de Bitcoin, por ejemplo, que el emisor tenga fondos suficientes.

6.
Con el bloque publicado en la cadena de bloques, los nodos de la red actualizan los saldos de bitcoin que hay en cada dirección.

7.
Cada vez que un bloque se agrega a la cadena de bloques, suma una confirmación a cada transacción de los bloques anteriores.

Cada bloque toma diferente tiempo en minarse, la importancia de que sean 10 minutos es por seguridad. Conforme avanza la tecnología y aumente la cantidad de mineros, se dificulta el hashing de los bloques de la red Bitcoin, ya que de lo contrario, si el problema matemático tuviera la misma dificultad, cada vez sería más fácil de resolver. Otra razón por la que unas toman más tiempo que otras es debido a que los mineros priorizan según la suma de tarifas que tiene el bloque. Cuando se ingresa la tarifa al iniciar una transacción de bitcoin, es importante pensar que mientras más baja se configure esta, menos incentivo tendrán los mineros de procesarla. Entonces tardará más en completarse ya que las tarifas ingresan a bloques según el rango de tarifa de cada uno y los mineros escogerán al que más les pague en tarifa.

Figura 7.3: Segunda extensión de la explicación de *Bitcoin*

Conoce Más

Ahora Veamoslo

Si quieres ver a la red Bitcoin en acción, puedes usar un explorador de bloques para ver todo lo recién explicado funcionando. A continuación usaremos uno llamado "mempool" **aquí**, para demostrar partes de lo explicado.

Figura 7.4: Tercera extensión de la explicación de *Bitcoin*

A continuación se podrán observar la extensión de *Lightning Network*:

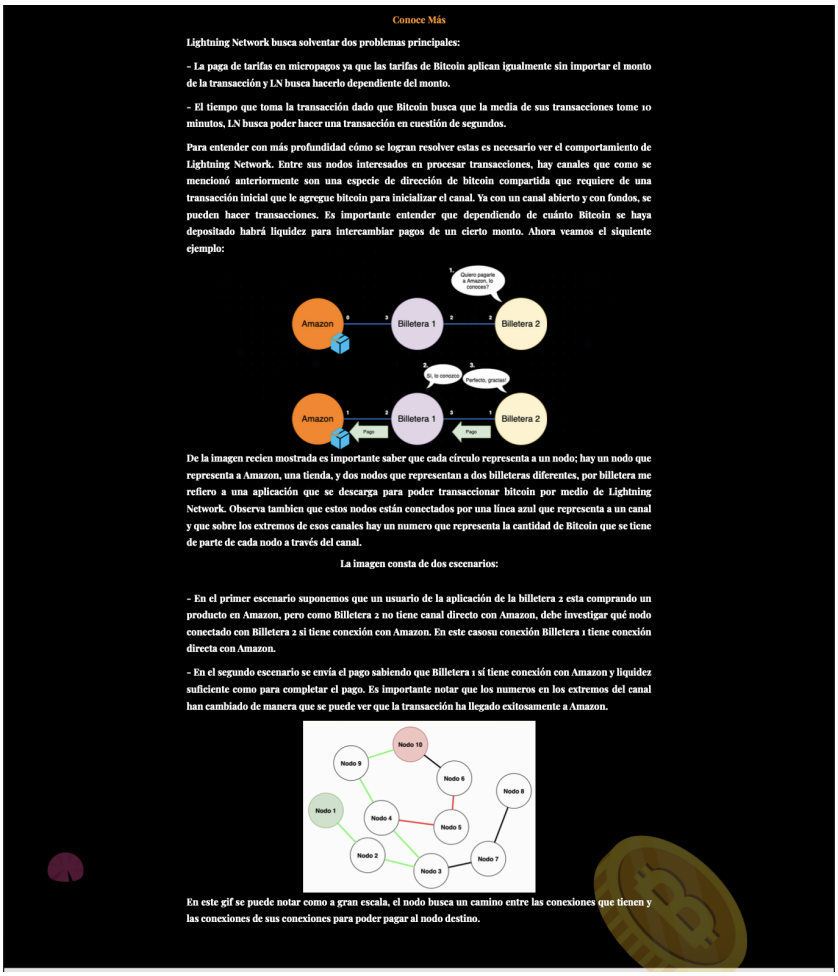


Figura 7.5: Primera extensión de la explicación de*LN*

Para finalizar la guía presenta un reto a completar, especialmente para programadores. Explica los pasos a seguir y hay un botón que lleva al repositorio del reto donde está documentado cómo empezar.

Figura 7.6: Presentación del reto

En cuanto a los resultados del desafío que muestra el funcionamiento del método de pago de *Lightning Network* a través de una historia en la cual se ayuda a Lisa, un personaje ficticio dueño

de una cafetería en la Universidad del Valle de Guatemala a configurar los nodos de sus clientes y proveedores. Se realizó una especie de dibujos para cada uno de los personajes, incluso para poder reflejar las acciones que se hacían y facilitar la comprención del programa. Para hacer uso de *Polar*(un emulador de nodos de *Lightning Network*) se usaron varios recursos como manuales [7] [18] [19] y repositorios [20] [21]

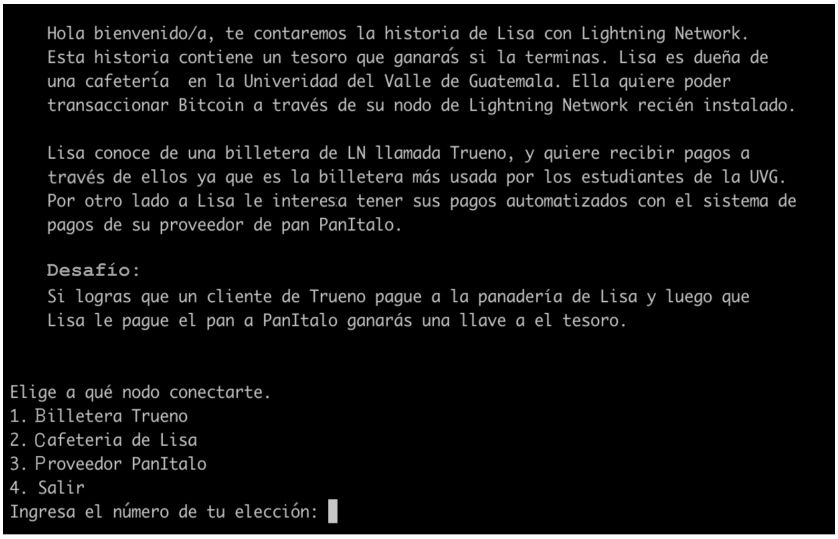


Figura 7.7: Primer menú

Figura 7.8: Abrir un canal

Figura 7.9: Hacer un cobro deLN

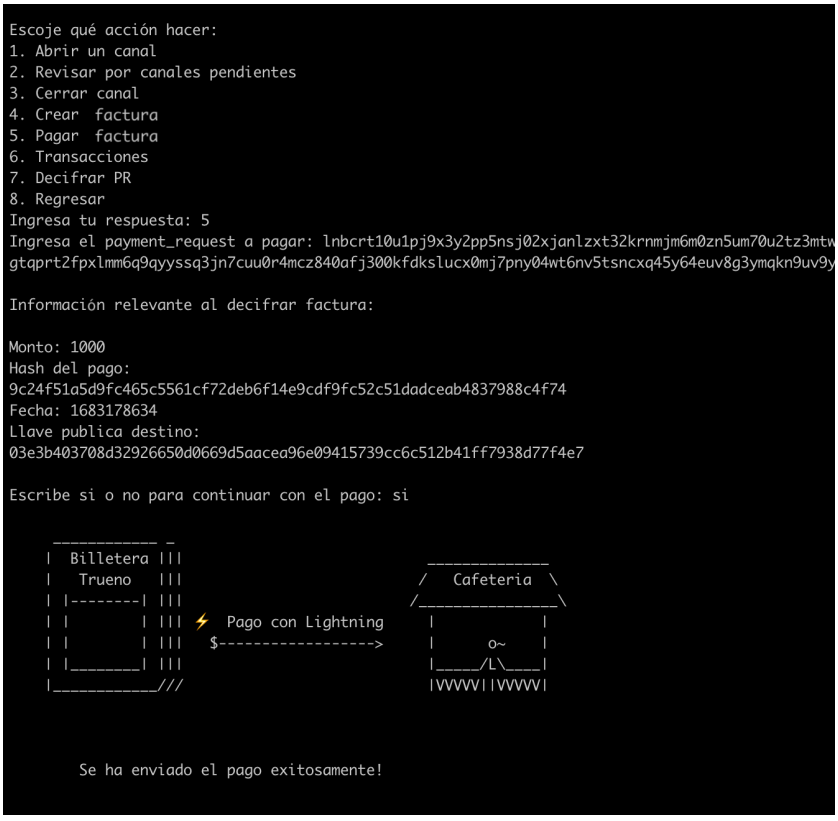


Figura 7.10: Pagar el cobro deLN

7.2. Resultados de entrevistas y encuestas sobre la guía de *Bitcoin*

En el marco de esta investigación, se llevaron a cabo entrevistas y encuestas con el objetivo de obtener información respecto a la comprensión detallada y generalizada sobre la guía de *Bitcoin*.

7.2.1. Metodología de la encuesta:

Se seleccionó un amplio grupo de personas mayores de 18 años con al menos un título de colegiatura, y con interés en aprender sobre Bitcoin. De entre los seleccionados, 5 personas cumplían exactamente con el *user persona* mencionado anteriormente. La encuesta se diseñó de manera que los participantes pudieran leer la guía a su propio ritmo antes de responder a las preguntas proporcionadas. En total, se recopilaron 11 respuestas, de las cuales 5 se obtuvieron mediante entrevistas directas. Los perfiles de los entrevistados incluyeron:

- Dos profesionales de 23 años con experiencia en informática y *Bitcoin*.
- Un joven bachiller de 18 años que ha oído hablar de *Bitcoin*.
- Una profesional de 23 años con conocimiento de *blockchain* y cierto nivel de familiaridad con *Bitcoin*.
- Una profesional de 36 años con que ha oído hablar de *Bitcoin*.

7.2.2. Resultados de encuesta:

A continuación, se presentan los resultados más destacados obtenidos a partir de las encuestas y entrevistas:

- Lectura de la Guía: Todos los 11 encuestados leyeron la guía en su totalidad.
- Comodidad de lectura:

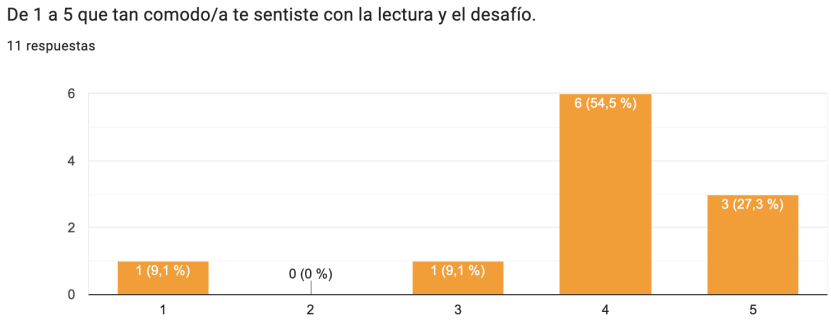


Figura 7.11

- Dudas después de la lectura: Algunos participantes manifestaron dudas después de leer la guía, incluyendo la necesidad de una explicación más clara sobre la conexión de*LN*, la definición de *hashing*, dificultad para entender cómo funcionaban los botones expansibles, la sugerencia

de incluir un índice o el propósito de la guía, proporcionar una introducción a *Bitcoin* y su funcionamiento actual, y señalar que había términos técnicos que requerían una mayor explicación.

- Cambios de diseño sugeridos: Los cambios de diseño sugeridos incluyeron el cambio de tipografía (solicitado por 4 personas), la incorporación de más imágenes y menos texto (solicitado por 3 personas), mejorar el estilo de los botones (solicitado por 3 personas), y una mejor separación entre texto e imágenes (solicitado por 2 personas).
- Disposición a compartir la guía: 9 de los 11 encuestados expresaron su disposición a compartir la guía con otros.
- Comentarios y sugerencias finales: La sección de comentarios y sugerencias reveló que los participantes observaron faltas de ortografía, sugirieron hacer la guía más dinámica, reemplazar términos en inglés por equivalentes en español (o utilizar comillas para destacarlos), y hacer que la presentación sea más visual.

Durante las entrevistas, también se indagó sobre la comprensión de la relación entre *Bitcoin* y *Lightning Network*, así como sobre la definición de cada uno. De los 5 entrevistados, 4 respondieron correctamente a la pregunta sobre la conexión, explicando que a través de los canales de *Lightning*, *Bitcoin* es necesario tanto para abrir como para cerrar un canal, ya que se requiere una transacción de apertura y otra de cierre para equilibrar los saldos. En cuanto a la definición de *Bitcoin*, los 5 respondieron de manera adecuada, destacando sus características y cualidades, enumerando al menos 3 cualidades y 2 características distintivas. Sin embargo, respecto a la definición de *Lightning Network*, solo 3 de los 5 entrevistados ofrecieron respuestas correctas, describiéndola como una red de nodos que utiliza *Bitcoin* para asegurar las transacciones entre sus canales.

Conclusiones:

- A través de las entrevistas, se confirmó que la guía proporciona una explicación efectiva sobre la relación entre *Bitcoin* y *Lightning Network*, así como sobre las definiciones de cada uno.
- Varios de los entrevistados expresaron que encontraron la guía como una forma innovadora de obtener información.
- La guía resultó ser interesante para todos los encuestados; de los 11 participantes, 9 la leyeron en su totalidad, mientras que solo el resto omitió una sección de las 10 disponibles.
- Los resultados de la guía mostraron una necesidad de trabajo mayormente en detalles como imágenes, simplificación de texto y correcciones ortográficas.
- Se observó que se requiere una mayor claridad y elaboración en la redacción de la conexión entre *Bitcoin* y *Lightning Network*, a pesar de que 4 personas lograron comprender la explicación.

A continuación se describen las acciones que se llevarán a cabo para la siguiente versión de la guía.

- Mejorar botón de “Conocer Más”.
- Corregir faltas ortográficas.
- Agregar imágenes que ayuden a entender los mensajes escritos.
- Simplificar mensajes (evitar redundar), para reducir el texto.
- Usar un estilo de fuente general fácil de leer.
- Agregar hipervínculos a palabras tecnicas que no se expliquen.
- Explicar palabras técnicas importantes.
- Agregar visualización de *Lightning Network*.

7.2.3. Resultados de entrevistas:

En cuanto al código de desafío, se obtuvieron los siguientes comentarios de dos programadores participantes:

- El readme no tiene suficientes recomendaciones al tener problemas con la instalacion de docker (los entrevistados proporcionaron los links que ellos usaron para resolver ciertas dependencias).
- Se descubrió que en el caso de IOs Mac ya no se incluye docker-compose en Docker Desktop. Es una actualización desde julio del 2023.
- Hay un poco de desorden en las instrucciones, ya que pide cambios en el código y después clonarlo, debería de pedir que lo clone antes.
- A pesar de haber una sola instalación de *python*, siempre es recomendable facilitar un ambiente que automáticamente se ejecute solo.
- *Polar* no reconocía docker a pesar de tenerlo instalado, pero logré solucionarlo(compartió el link con el que resolvió el problema).
- No sé cómo minar bloques(se tuvo que instruir).
- En el desafío hay instrucciones clave que me pudieron haber ayudado a entender cómo saber cuántos bloques minar para que se active el canal, tambien explicar que sin canal la transacción no llega.
- Me resultó difícil la lectura de ciertos mensajes, ya que se perdían entre otros mensajes, recomiendo usar *input* es *python* para que se hagan las pausas de lectura.
- Algunos errores causaban confusión (compartió que error fue el más confuso).
- Al resolver el desafío, se repite el mensaje de éxito 3 veces.

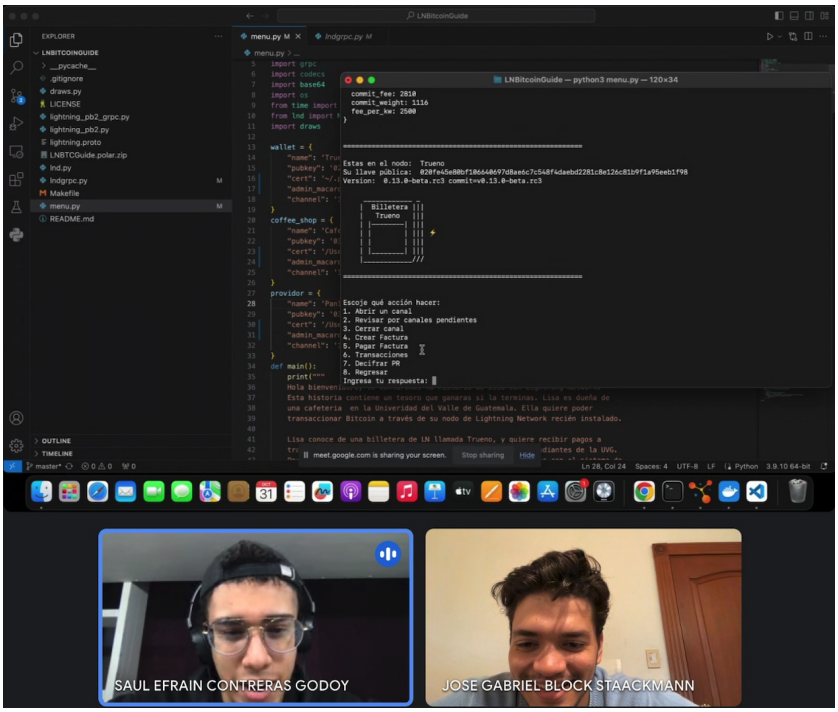


Figura 7.12: Evidencia de una entrevista

Conclusiones: Estas son las acciones que se llevarán a cabo luego de analizar los resultados de las entrevistas.

- Se captó una actitud de alegría de ambos entrevistados, ambos mostraron emoción al ver los dibujos y sentir el reto a completar.
- Ordenar documentación y mejorar la explicación.
- Agregar links de ayuda para facilitar instalación.
- Se agregará color a los textos dependiendo del tipo de mensaje. Se confirmó una manera de hacerlo en *python* sin agregar dependencias.
- Agregar especificación en errores, se pintarán de rojo.
- Agregar pistas importantes a pagar factura, hacer factura y abrir canal.
- Arreglar mensaje de éxito del desafío, ya que se repite 3 veces.
- Considerar facilitar un ambiente que se ejecute con bash.

7.3. Examen final

Se realizó un examen con cuatro preguntas a los dos desarrolladores de 22 a 25 años que leyeron la guía y completaron el desafío:

- Escriba con sus palabras qué es Bitcoin.
- Escriba con sus palabras qué es Lightning Network.
- Justifique cuál es la conexión de Bitcoin con Lightning Network.
- ¿Qué es LNURL y qué implica?

A estas preguntas ambos examinados respondieron correctamente todas las preguntas.

Conclusiones:

- Se pudo reafirmar con claridad que ambos examinados aprendieron lo necesario para contestar las preguntas anteriores.
- Se observó que quizás hay pequeños detalles que necesitan una mayor aclaración, pero dado que son aspectos que no tienen un gran impacto en los objetivos de este proyecto, no se realizarán modificaciones. Es importante mencionar que no pudieron responder cuando se les preguntó si realizarían cambios en la guía o en el desafío.

7.4. Guía beta

Se puede decir que este es el resultado final. A continuación se mostrará la segunda version del proyecto completo. Para esta ocación, se ha publicado el proyecto. Este se puede ver en el siguiente subdomino: https://bitcoin-guide.tecnitrain.com/. Se verificó y extendió todo el contenido de la guía que pudiera causar mucha confusión. Se modificó el botón de "Conocer Más" a "Leer Más". Se agregaron imágenes y videos a ciertos textos. Se agregó una sección que explica *LNURL* en pocas palabras y una extensión de *Lightning Network* que muestra y explica a la red en tiempo real en el mundo.

7.4.1. Comentarios:

Se presentó la guía beta a varias personas para escuchar sus comentarios e intereses en la guía. A continuación los comentarios:

- Me gusta mucho la variedad de medios que se usan para explicar diferentes temas.
- Me desanimó que dijera "Leer más" despues de una imagen, pensé que iba a hablar más de la imagen. Luego noté que no habla de la imagen sino que continúa explicando y me gustó. (Fue un comentario de una sola persona)
- Entendí mejor que es *Bitcoin* y *Lightning*.
- Es bastante vistosa, considero que hay más por hablar, pero los parrafos conectan de manera que si entendí pero me quedo con más dudas de ambos temas.
- Una buena comparación de hacer *Lightning Network* con el sistema de vuelos internacionales.

En conclusión, se considera que eventualmente los temas podrían expandirse, pero alojándolos en otra página dentro del mismo subdominio. También se intentará resolver la problemática relacionada con el botón "Leer Más".

Por último, se realizó una presentación del código final, del cual se ha creado un video que muestra la resolución del desafío planteado: https://youtu.be/hFjVGSeKJ6Y. Al completar el desafío, se utiliza una llave en la guía para desbloquear un cobro *LNURL* durante un tiempo determinado, permitiendo posteriormente su consumo y la obtención de 1000 *Sats* o 0.00001000 *bitcoin*.

CAPÍTULO 8

Conclusiones

1. El objetivo principal se logró satisfactoriamente, ya que en las entrevistas y encuestas, los participantes fueron capaces de explicar con éxito la relación entre *Bitcoin* y *Lightning Network* después de consultar la guía.

2. Se cumplieron los objetivos de definir *Bitcoin* y *Lightning Network* con precisión, así como demostrar la funcionalidad de *Lightning Network*. Todos los entrevistados demostraron comprender *Bitcoin* y sus capacidades en las entrevistas y encuestas gracias a la guía. Varios expresaron comentarios positivos, especialmente cuando se utilizaron ejemplos cotidianos para ilustrar los conceptos.

3. Se proporcionó una explicación exitosa de *LNURL* y cómo mejora la experiencia del usuario, ya que en el examen final los participantes pudieron responder correctamente a su definición.

4. Se creó con éxito un repositorio educativo sobre *Lightning Network* en *GitHub*.

5. Se observó a varios programadores ejecutar el repositorio sin necesidad de asistencia adicional.

CAPÍTULO 9

Recomendaciones

1. Se recomienda visitar el enlace a la guía para obtener una comprensión más profunda de los temas discutidos en este informe.
2. En general, se aconseja una lectura completa de la guía beta, incluso si surgen dudas, ya que es probable que se encuentren las respuestas a medida que se avanza.
3. A quienes deseen dar seguimiento a la guía y el desafío, se recomienda mantenerse al día con la información y explorar las nuevas tecnologías emergentes en *Bitcoin*, como *LN-Address*, y considerar la posibilidad de agregar desafíos más complejos, como la incorporación de *LNURL*.
4. A aquellos interesados en implementar *Lightning Network* se recomienda utilizar las referencias como punto de partida, ya que el repositorio del desafío podría no estar actualizado con la versión más reciente.
5. También se sugiere a los interesados en implementar *Lightning Network* que realicen una investigación sobre el protocolo de nodo más popular y robusto. En este momento, *LND* es una opción, pero se recomienda verificar que la tecnología no haya cambiado.
6. Es importante recordar que, aunque podría haberse utilizado una interfaz de usuario en el proyecto, se optó por una implementación en línea de comandos con fines educativos.
7. Para aquellos interesados en impactar en la educación, se les invita a participar en el proceso de mejorar los recursos educativos sobre cualquier tema de su elección.

CAPÍTULO 10

Bibliografía

[1] I. Blockchain, "¿Qué es la tecnología blockchain?" *https://www.ibm.com/es-es/topics/blockchain*,

[2] A. M. Antonopoulos, *Mastering Bitcoin*. gitHub, 2021.

[3] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin Network, inf. téc., 2008.

[4] "The Bitcoin Lightning Network:Scalable Off-Chain Instant Payments," Lightning Network, inf. téc., 2016.

[5] B. Academy, "Guía para Principiantes sobre la Lightning Network de Bitcoin," *https://academy.binance.com/es/is-lightning-network?utm$_s$ource = googleadwords$_i$nt&utm$_m$edium = cpc&ref = HDYAHEES&gclid = Cj0KCQjwmICoBhDxARIsABXkXlKRO8Onpg6K52MZKsguTnESdCSz14tBBtRKNzq84sH−OQx$_2$NayRb8aAtFGEALw$_w$cBheader − 4*, 2018.

[6] B. Academy, "¿Qué son los nodos?" *https://academy.binance.com/es/articles/what-are-nodes*, 2018.

[7] *Lightning Network Daemon*, 2015.

[8] Voltage, "LNURL – ENHANCING LIGHTNING'S USER EXPERIENCE," *https://voltage.cloud/blog/lightning-network-faq/how-does-lnurl-work-enhancing-lightnings-user-experience/*, 2023.

[9] Unimooc, "Bitcoin: definición y características," *https://unimooc.com/bitcoin-definicion-caracteristicas*, 2015.

[10] Coinbase, "What is the Lightning Network?" *https://www.coinbase.com/es/learn/crypto-basics/what-is-lightning*, 2022.

[11] B. Academy, "¿Qué es el Hashing?" *https://academy.binance.com/es/articles/what-is-hashing*, 2023.

[12] *Watchtowers*, 2022.

[13] C. Campbell, *Who sets the Bitcoin price? | Bitcoin price differences explained*, `https://www.youtube.com/watch?v=FI_YCS3MERE`, ene. de 2018.

[14] C. Professor, *How Do Cryptocurrencies Work Gain Value? | Cryptocurrency Explained For Beginners | CP BW*, `https://www.youtube.com/watch?v=8VSztCUbvQw`, nov. de 2020.

[15] L. S. Bitcoin, *Cyphernode, Lightning Network and LNURL*, `https://www.youtube.com/watch?v=M1ZLka0j0Tg`, sep. de 2021.

[16] L. fiatjaf, *LNURL Documents*. gitHub, 2021.

[17] *Mempool*, `https://mempool.space/`.

[18] *LND API reference*, 2023.

[19] *LND Builder's Guide*, 2022.

[20] L. Network, *How to write a Python gRPC client for the Lightning Network Daemon*, `https://github.com/lightningnetwork/lnd/blob/master/docs/grpc/python.md`, 2020.

[21] L. Network, *Lightning Network In-Progress Specifications*, `https://github.com/lightning/bolts/blob/master/00-introduction.md`, 2019.

CAPÍTULO 11

Anexos

11.1. Repositorio

A continuación se presenta el repositorio del reto para montar un nodo local y cumplir con la historia: https://github.com/joseblock/LNBitcoinGuide

CAPÍTULO 12

Glosario

Hashing: el proceso de tomar una entrada (o 'mensaje') y devolver una cadena de caracteres fija de longitud, que generalmente parece ser un valor alfanumérico aleatorio. [11]. 38

Inflación: la inflación es un fenómeno económico que se observa en un país se ve directamente relacionado con el aumento desordenado de los precios de la mayor parte de los bienes y servicios que se comercian en sus mercados, por un periodo de tiempo extendido.. 38

LN Watchtowers: entidades que protegen los canales de Lightning Network contra posibles fraudes, monitoreando y respondiendo a actividades sospechosas en la red. [12]. 38

Nodo de Lightning (LND): una implementación completa de un nodo de la Red Lightning que permite crear canales, cerrar canales, gestionar estados del canal y más.. 38

Open-source: conocido también como "Código Abierto", es un código diseñado de manera que sea accesible al público. Se desarrolla de manera descentralizada y colaborativa para hallar la manera de solucionar los problemas en conjunto.. 38

Peer-to-peer: es una red de pares. Consiste en un modelo de comunicación descentralizado, es decir, no necesitamos un servidor central, sino que cada parte o usuario actúan por igual y pueden tener la función de servidor o de cliente. Consiste en un modelo de comunicación descentralizado, es decir, no necesitamos un servidor central, sino que cada parte o usuario actúan por igual y pueden tener la función de servidor o de cliente.. 38

Protocolo: es un conjunto formal de estándares y normas. Rigen tanto el formato como el control de la interacción entre los distintos dispositivos dentro de una red o sistema de comunicación.. 38

Red: se le conoce así a las series de ordenadores o dispositivos informáticos que se conectan por medio de cables, ondas, señales u otros mecanismos con el propósito de transmitir datos entre sí, además de recursos y servicios, con el fin de generar una experiencia de trabajo compartida, y ahorrar tiempo y dinero.. 38