

Taller de Proyecto II

2020

Plan de Proyecto

PS 6: Investigación sobre Blockchain

Grupo de Desarrollo

- Gamal Lascano Hassen - 1279/2
- Corsino Alexandre - 01699/9

Informe de Avance 26/10/19

0.- Blockchain

Blockchain, como se describió en el informe anterior, consiste de un registro único, consensuado y distribuido entre varios nodos en una red, los cuales guardan en sí mismos información respecto al bloque mismo, y un vínculo al bloque anterior en la cadena, el cual no es modificable. A medida que se agregan nuevos registros, estos son verificados y validados por la red, y luego añadidos a un nuevo bloque que se enlaza a la cadena.

Como base, un bloque tiene un índice, una timestamp que indica el momento en que se crea el bloque, una transacción, la cual contiene información del que envía y recibe el bloque, con la cantidad que se quiera enviar, luego tiene un hash como prueba y un link al hash previo.

Cuando se crea una instancia de una blockchain, se la necesita instanciar con un bloque génesis, o sea, el primer bloque, el cual no tiene predecesores. El chequeo utilizado para crear nuevos bloques o minar se llama Proof of work. Proof of work es un algoritmo que intenta descubrir un número que solucione un problema. El número debe ser difícil de encontrar pero fácil de verificar por cualquier nodo en la red. El número a solucionar está atado a condiciones establecidas por el creador de la red, por ejemplo: Que el hash entre dos números termine en 0.

Casos de uso

Control de cadena de suministros, Identidad digital, Mercado inmobiliario, Sector de la salud, Sistemas de votación, Criptomonedas.

Control de la cadena de suministros: Todos los activos en la cadena de suministro deberán digitalizarse, pero cada producto, una vez digitalizado, tendrá un número de serie único asociado al mismo. Por lo tanto, cada activo puede ser monitoreado y rastreado a través de la cadena de suministro, en conjunto con otra información asociada al mismo que se quiera conocer. Ejemplo: Food Trust de IBM.

Identidad digital: Forma de tener una fuente confiable para sistemas gubernamentales de verificar la identidad de cierta persona. No es susceptible a robo de identidad de esta manera. Ejemplo: Hyperledger Indy
Sistema de salud: Sirve para el almacenamiento de datos sanitarios de una persona en una red descentralizada, por lo cual se puede tener consistencia entre múltiples hospitales o establecimientos de salud. Ejemplo: SimplyVital health

Mercado Inmobiliario: Sirve para el pago de alquileres o compras de propiedades.

Ejemplo: propy

Sistema de votación: Usando la identidad única de cada persona, se puede votar de forma segura desde cualquier lugar, llevando a múltiples ventajas: Eliminación del fraude electoral, verificación de votos, almacenamientos de votos seguros en la red como blockchain y aumento de confianza y transparencia.

Criptomonedas: El uso tradicional de la tecnología blockchain. Facilita las transacciones entre pares, elimina a posibles intermediarios y sirve como alternativa monetaria a servicios de billetera online. Ejemplos: Bitcoin, Ethereum

1.- Proyecto

Objetivo original

El objetivo original de este proyecto es realizar una blockchain con el propósito del seguimiento de objetos. Se le asigna un código a un objeto en específico, el cual se podrá escanear para poder recuperar la información actual y pasada del mismo. Asimismo se dispondrá de una página web para poder agregar nuevos objetos a la blockchain. Para enviar los datos de los objetos, contaremos con una placa arduino conectada a una red wifi, la cual manda la información de los objetos a una página web.

Modificaciones debido evaluaciones de la cátedra

Decidimos agregar una sección más en el informe para investigar más sobre la tecnología blockchain e investigaremos algunos proyectos.

Otras modificaciones

Decidimos sacar la placa arduino uno y conectar el scanner RFID a la placa NodeMcu directamente. De esta manera reducimos la complejidad de las comunicaciones sacando una línea i2c, logra facilitar el debugging y reducir la cantidad de líneas de código.

2.- Materiales y Presupuesto

Abajo se encuentra una tabla de los componentes utilizados, fueron comprados por mercadolibre:

| COMPONENTE | PRECIO (\$ARS) |
|---------------------|----------------|
| ESP8266 NODEMCU | 569 |
| ARDUINO UNO R3 | 949 |
| RFID RC522 | 269 |
| PROTOBOARD | 470 |
| CABLES M-M 30cm x10 | 46.8 |
| CABLE M-H 30cm | 7.75 |
| TOTAL | 2,311.55 |

Tab.1

3.- Esquema Gráfico del Proyecto

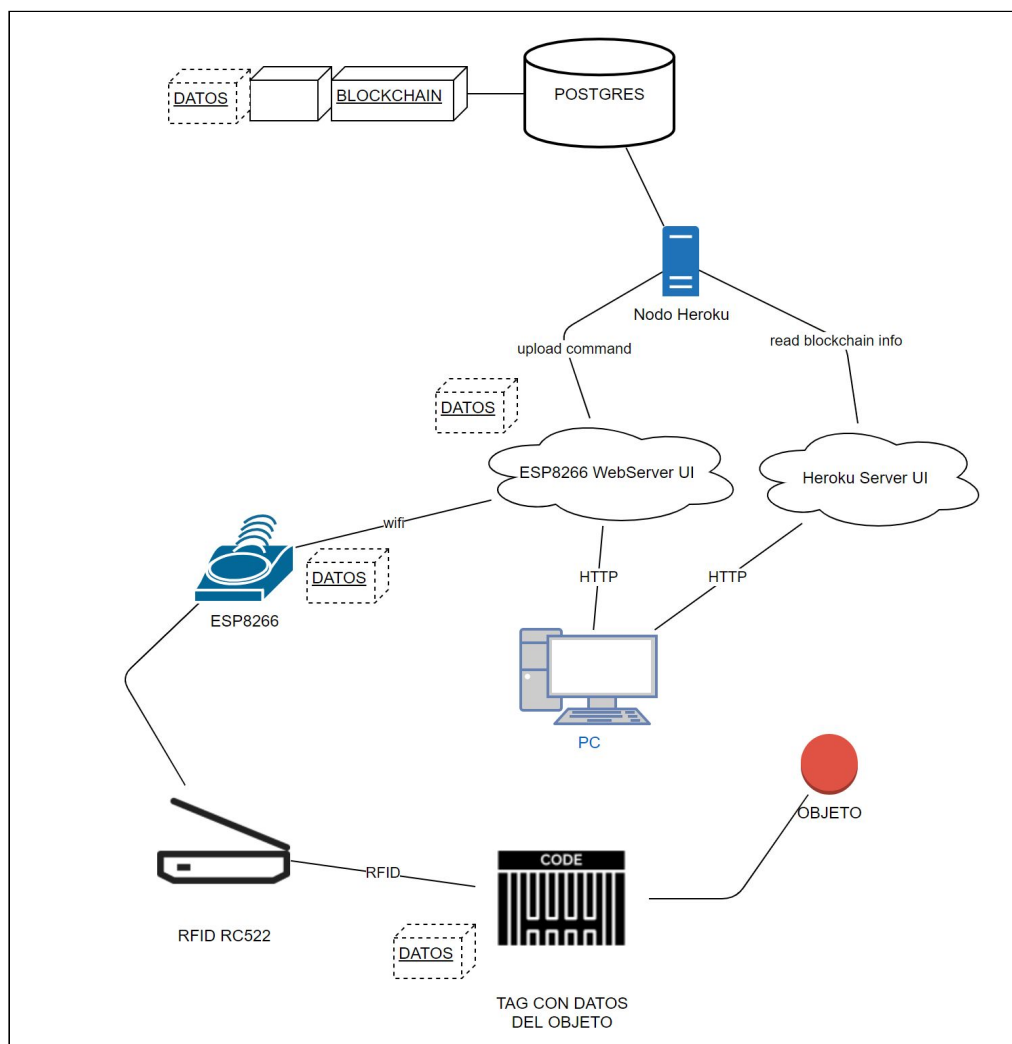


Fig.1: esquema actual del proyecto

ALIMENTACIÓN

Alimentación del ESP8266/Nodemcu (WiFi)

El módulo **ESP8266** es alimentado usando un cable y su puerto mini usb **V5**.

Alimentación del Rfid Rc522

El módulo **Rfid Rc522** es alimentado a través del NodeMcu por el pin **V3.3**

a) E/S del controlador/placa de desarrollo con el exterior, excepto PC

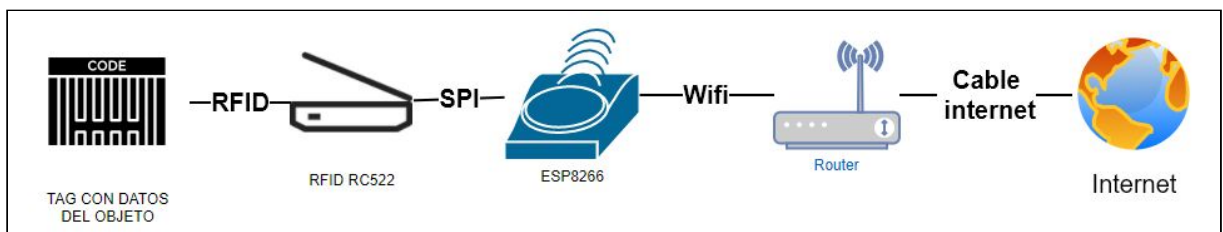


Fig.2: comunicación nodemcu a internet

SPI

El scanner rc522 se comunica con el nodemcu usando el protocolo SPI, permite comunicación sincrónica en un bus entre un maestro y múltiples esclavos.

SCLK es el pin reloj para mandar solo cuando hay un flanco alto de reloj, MOSI y MISO son pines master output slave input y master input slave output para determinar quien envia y quien recibe, SS es slave select para elegir el dispositivo a comunicar.

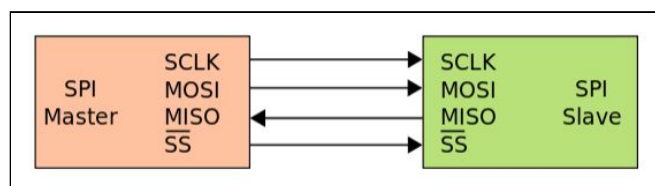


Fig.2b: protocolo SPI

b) Comunicaciones con la PC

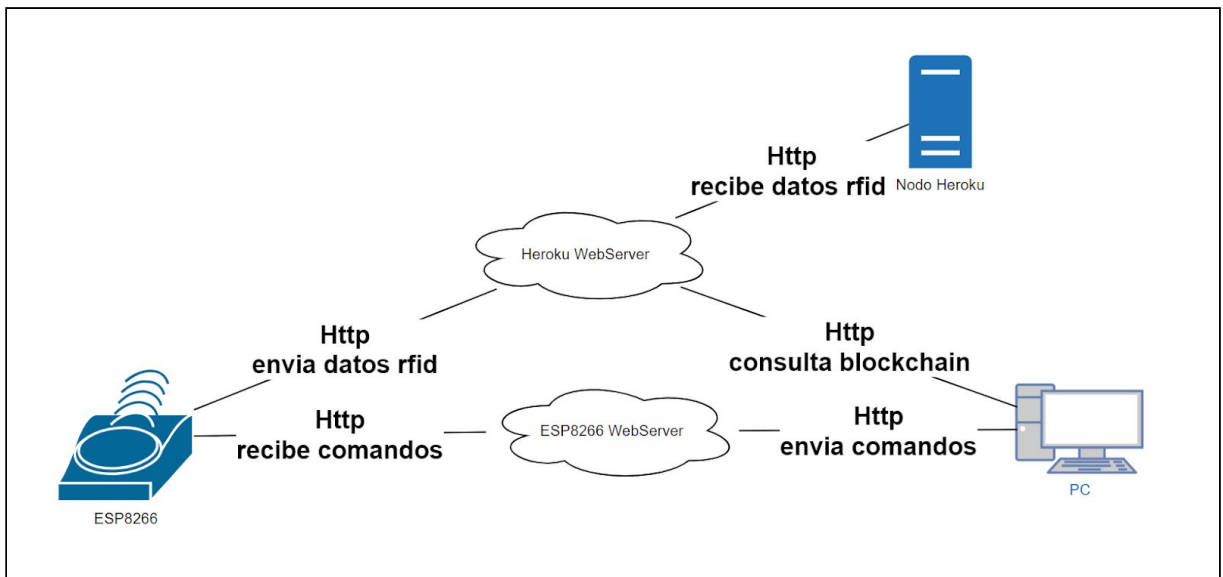


Fig.3: comunicación entre dispositivos

RFID RC522

El scanner rc522 sirve para escanear códigos RFID.

ESP8266

Esta placa nos permite instalar módulos y conectarse a una red wifi y luego internet para poder comunicarse con la pc y el sitio heroku.

HTTP POST y GET

El nodemcu utilizara el protocolo HTTP comando POST para mandar los datos rfid al sitio web heroku y para recibir comandos de la PC lo hará con HTTP GET.

SERVIDOR ESP8266

El sitio web del nodemcu nos permite controlar la placa mandando comandos. Los comandos esenciales son scan para escanear una tarjeta y upload para mandar los datos al sitio heroku.

SERVIDOR HEROKU

El sitio web estará hosteado en Heroku y dispondrá de una base de datos postgres donde se almacenará la blockchain.

c) Sistema web

HEROKU: Sitio web utilizado para el hosting y el mantenimiento del sitio web

NODEMCU SERVER: Sitio web utilizado para permitir la comunicación entre PC y Nodemcu

DJANGO: Framework utilizado para la realización de sitios web rápidamente, utilizado en conjunto con python

POSTGRES: Sistema de base de datos utilizado en conjunto con heroku para mantener la base de datos del sitio

PYTHON: Lenguaje de programación utilizado para programar el sitio web y la blockchain que mantiene el sistema

FLASK: API utilizada para implementar la blockchain en el sistema.

4.- Problemas y Soluciones

Hubieron varios problemas con relación al uso del repositorio github suministrado por la catedra e integraciones con aplicaciones de terceros. En nuestro caso particular, gitkraken y heroku. Uno de los integrantes del grupo usa gitkraken para administrar su repositorio, pero dado a que el mismo estaba dentro de la organización TP11, se necesitaba solicitar permiso al administrador del grupo para poder utilizar la herramienta. La solución a esto fue utilizar la CLI de git clásica, y realizar todos los commits a mano.

Lo mismo sucedió con heroku. Heroku tiene una integración la cual permite hacer un push automático a github de las cosas pusheadas a los servidores de heroku, sin tener que preocuparse que algún elemento esté desactualizado. En nuestro caso, tratar de conectar ambas herramientas resultó en la misma conducta que el primer punto. Nuestra solución fue separar a heroku y github en dos repositorios distintos. Todos los cambios hechos en heroku van a ser subidos a github cuando se hayan probado que funcionen.

Ahora tenemos 3 repositorios: el de heroku(heroku), el de la cátedra(tp11) y el de desarrollo (origin), la branch principal es: main.

5.- Documentación en Formato Gráfico y Video

Esquemas de hardware

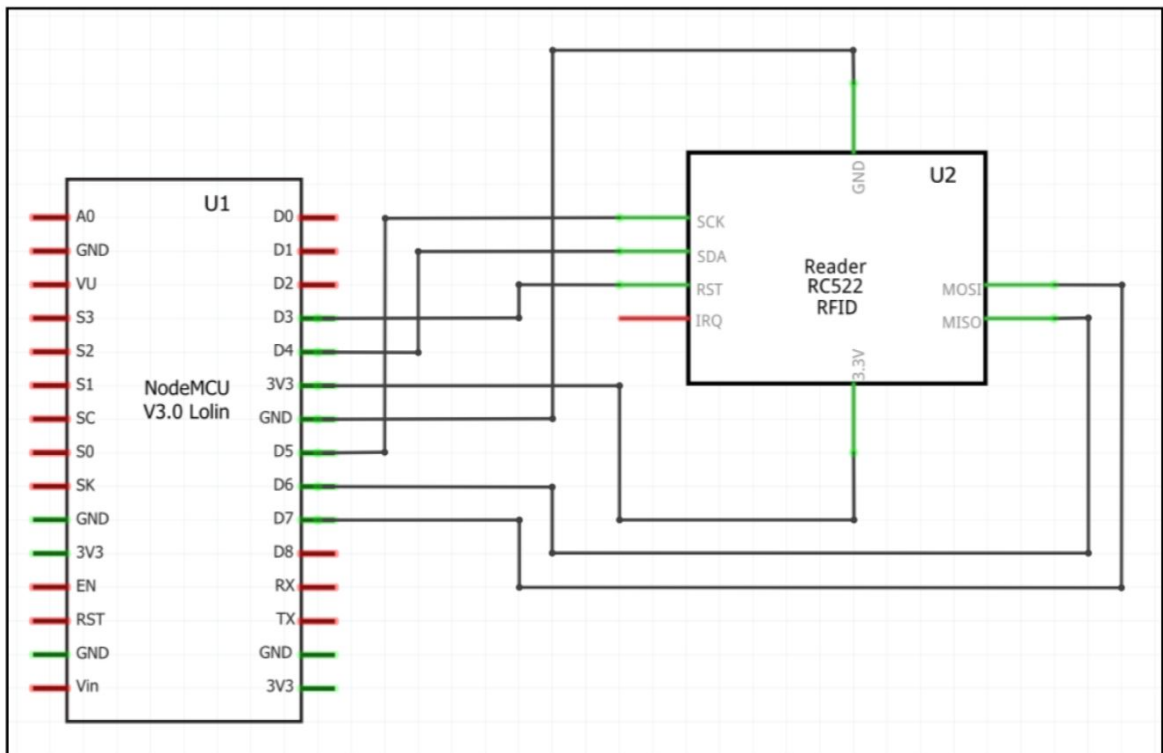


Fig.4: diagrama nodemcu y scanner

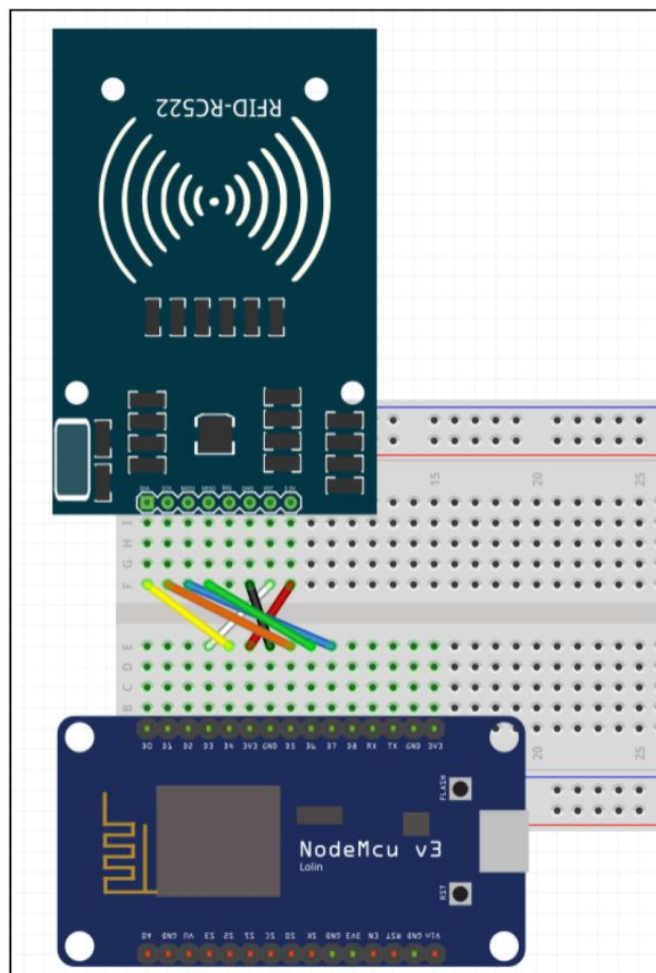


Fig.5: esquema nodemcu y scanner

Sistema físico actual

Foto del sistema, con el lector RFID conectado al nodemcu:

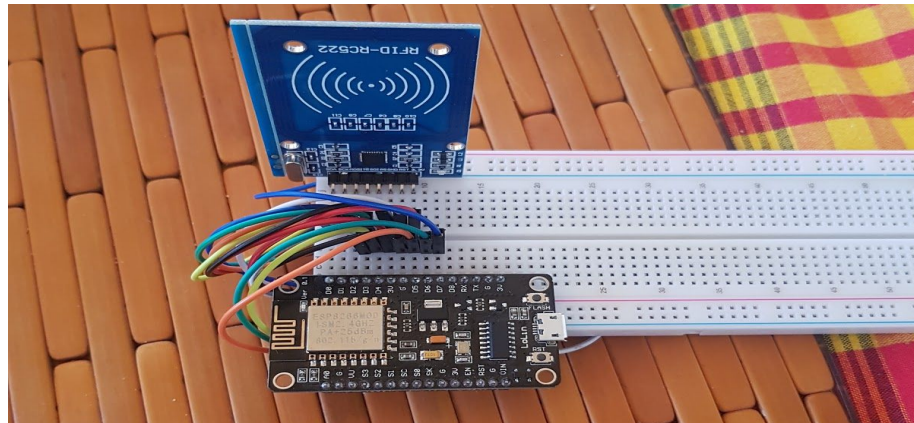


Fig.6: foto nodemcu y scanner

Video funcionamiento

Link de video mostrando el funcionamiento del lector RFID, junto con un sitio web:

<https://drive.google.com/file/d/1mUI2sNvmj7d6bKzBRr3AvVv3aaQ6qawT/view?usp=sharing>

Código nodemcu

Código Nodemcu: <https://codeshare.io/24DbQ3>