Bitcoin: Identificar nodos mineros

TRABAJO DE FIN DE MASTER

MÁSTER INTERUNIVERSITARIO DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES

Autor: Rubén Pérez Conte
Tutor: Cristina Pérez Solà

Índice

- Bitcoin
- Diseño
- Demostración
- Conclusiones y trabajos futuros

Bitcoin

¿Qué es Bitcoin?

- Más que una moneda.

- 2008 → inicio

- Robustez , anonimato, bajo coste, falta de control.

- 3,000 millones de €

Utilización

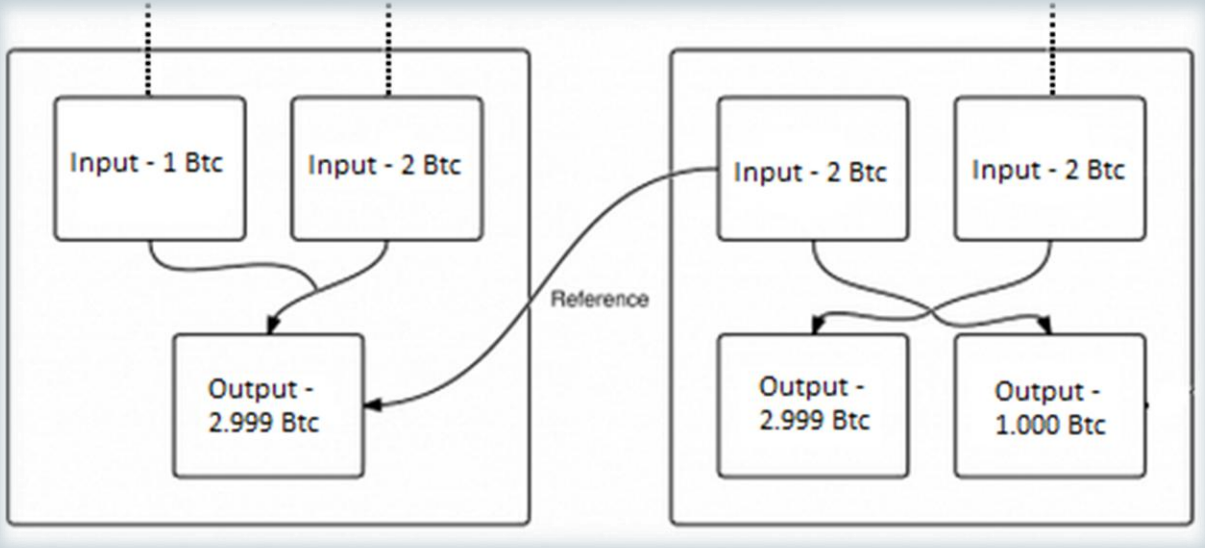
- Cliente
- Wallet
- Dirección
- Transacción

Dirección Bitcoin

1BfAZL5wT9sDX1C2tbA2gi2jZmRWnhzapr

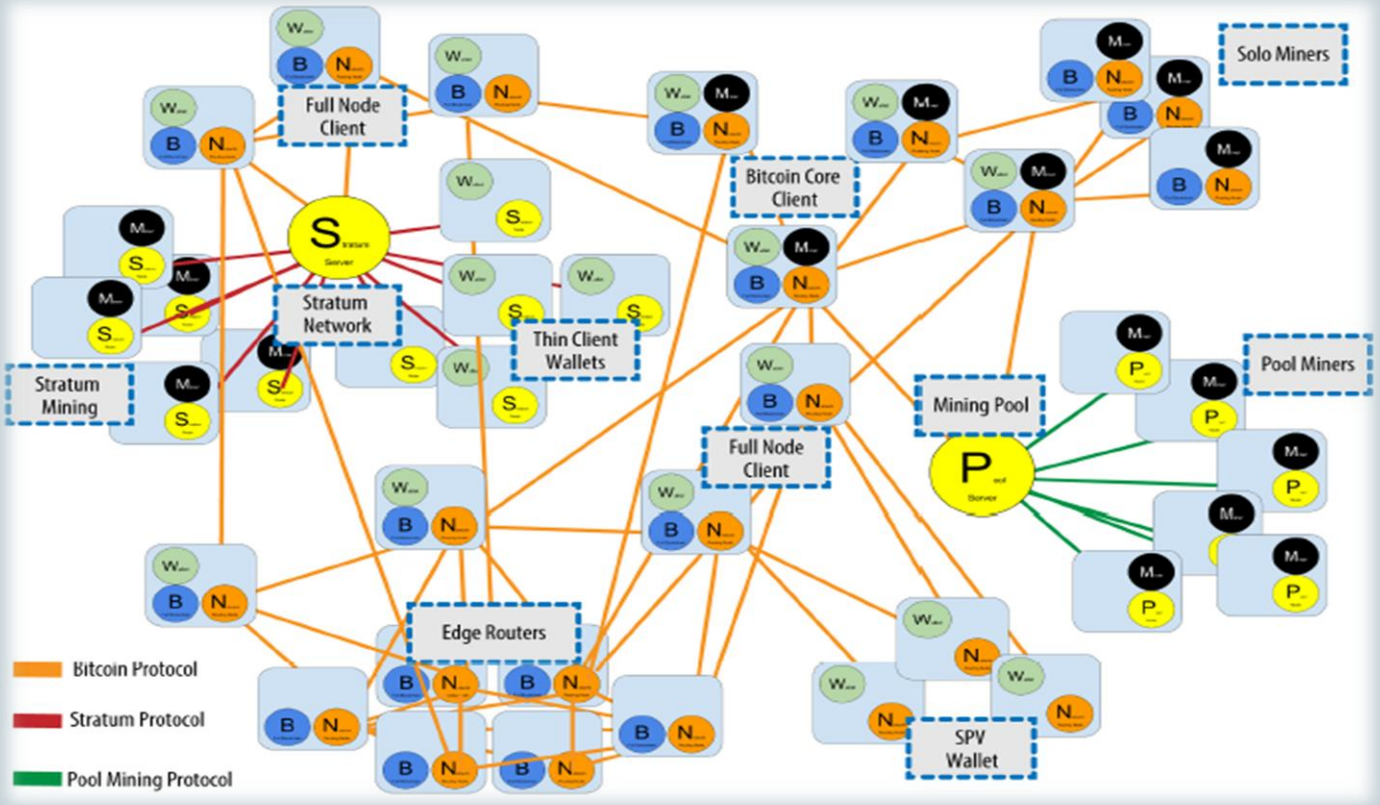
Clave privada

5Khr7KqV15kJesHFrvP2KDEEXA3yjqCiaDtWyn8MLtVPxyLWwwW



La red Bitcoin

- P2P de malla



Los Bloques y la Cadena de bloques

Bloque

- 5 Campos
- Cabecera
- Lista de transacciones

Cadena de bloques

- Bloques enlazados
- Consenso
- Seguridad

Minería

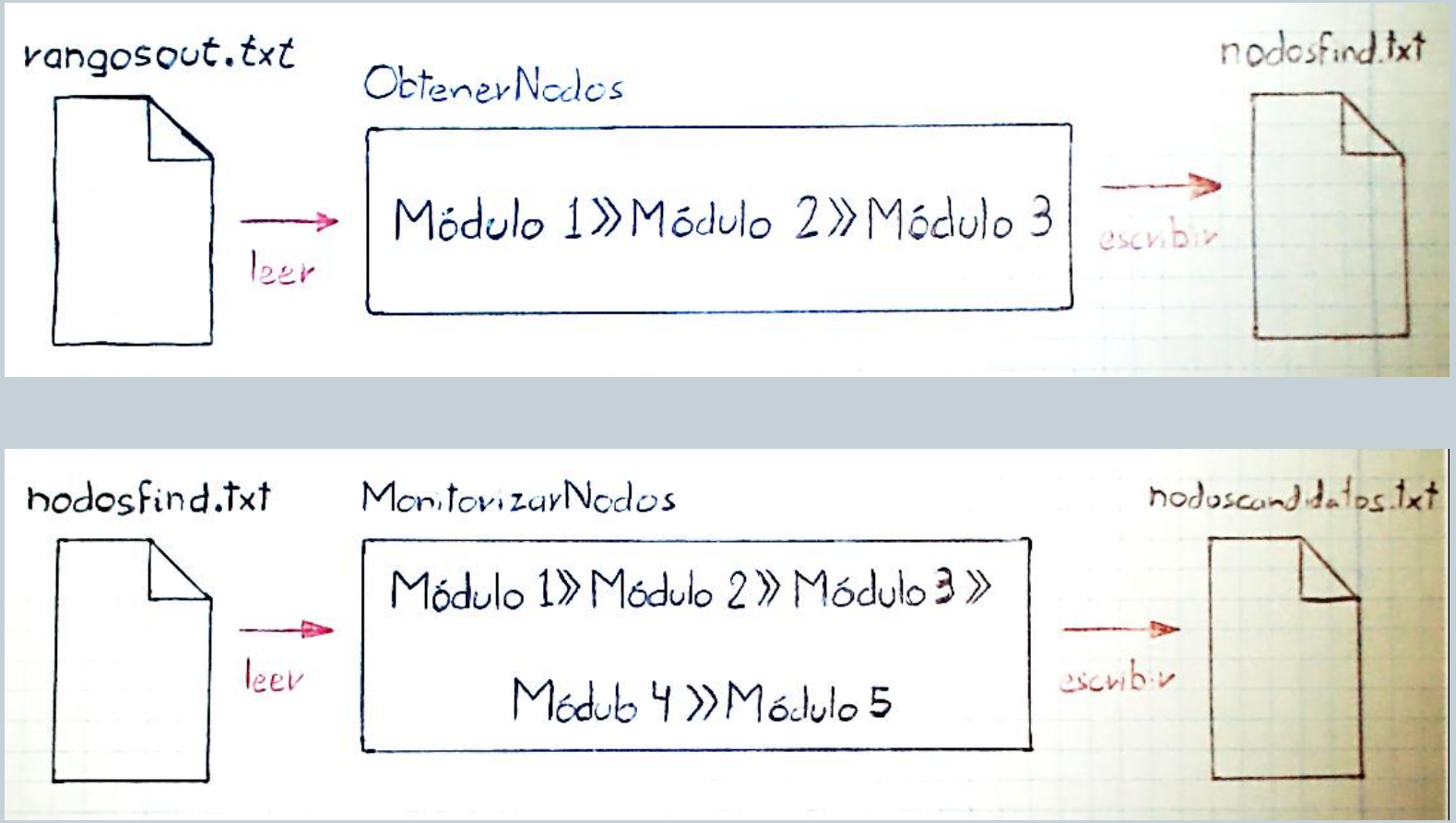
- Elegir transacciones
- Transacción generadora
- Construir cabecera
- Variar campos
- Realizar hash

Aplicación

Introducción

- Mineros accesibles
- Python
- Bitnodes y BitconSniffer
- 2 herramientas
  - ObtenerNodos
  - MonitorizarNodos

Esquema


rangosout.txt
leer
ObtenerNodos
Módulo 1 » Módulo 2 » Módulo 3
escribir
nodosfind.txt
nodosfind.txt
leer
MonitorizarNodos
Módulo 1 » Módulo 2 » Módulo 3 »
Módulo 4 » Módulo 5
escribir
nodoscandidatos.txt

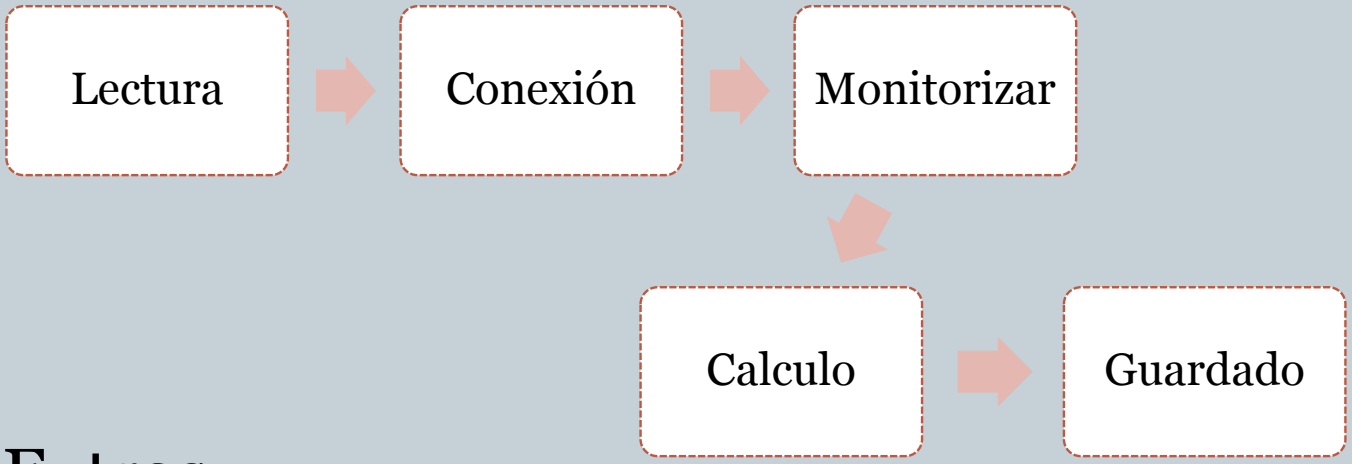
ObtenerNodos

- 3 módulos

- Extras
  - Log
  - Threads
  - Finalización

MonitorizarNodos

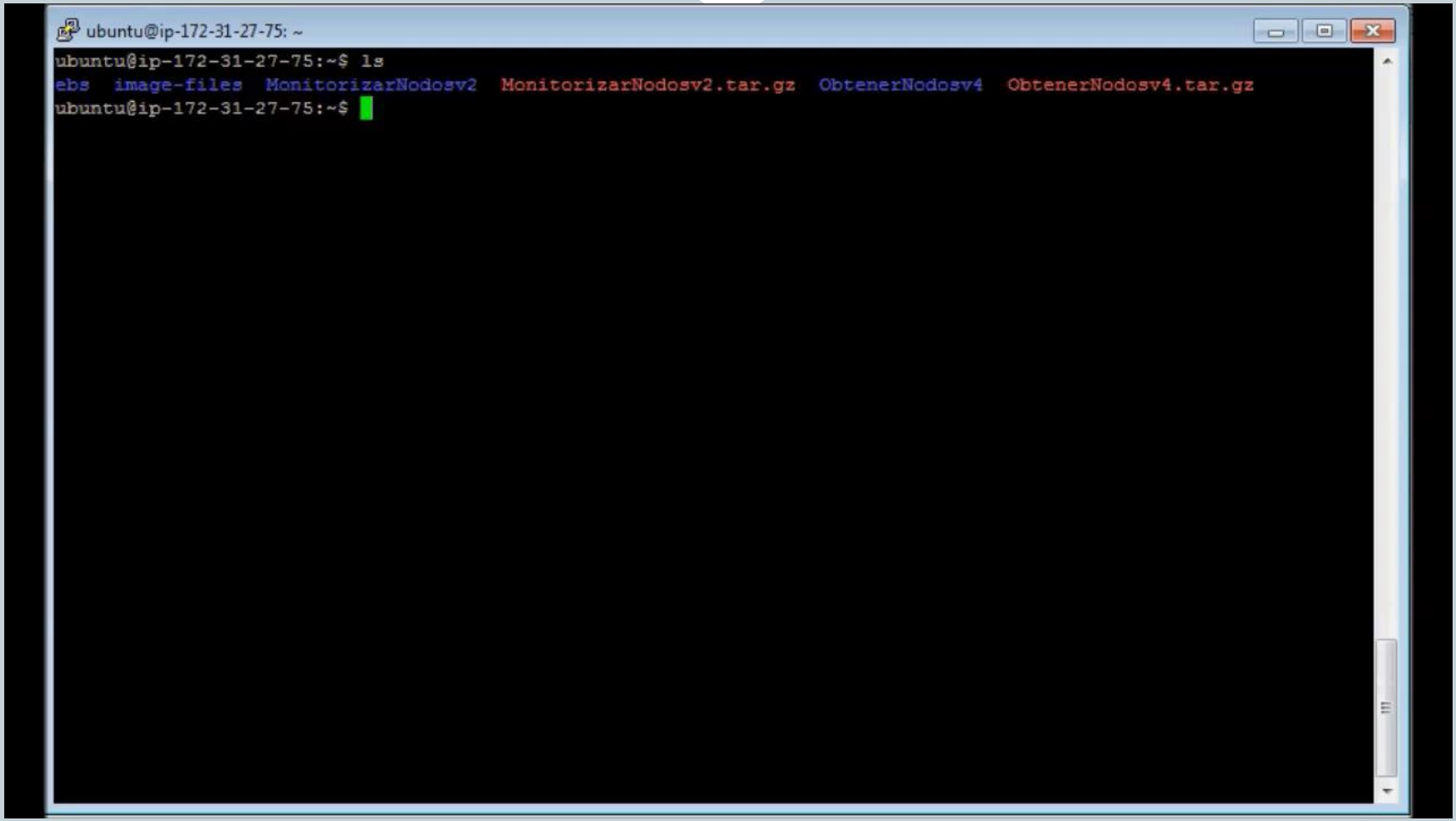
- 5 módulos



- Extras
  - Log
  - Threads
  - Finalización

Demostración

Video


ubuntu@ip-172-31-27-75: ~
ubuntu@ip-172-31-27-75:~$ ls
ebs image-files MonitorizarNodosv2 MonitorizarNodosv2.tar.gz ObtenerNodosv4 ObtenerNodosv4.tar.gz
ubuntu@ip-172-31-27-75:~$

Conclusiones y trabajo futuro

Conclusiones

- Conocimientos adquiridos altos
- Obtención de nodos lenta
- Monitorización deficiente
- No exito

Trabajos futuros

- Aumento del rendimiento
- Rediseño de las herramientas
- Objetivos secundarios
- Investigar en más detalle el sistema